(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 529 722**

(51) Int. CI.:

G01R 31/317 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.08.2012 E 12180652 (5)**

(97) Fecha y número de publicación de la concesión europea: **05.11.2014 EP 2574944**

(54) Título: **Iniciación de ataques en componentes de tarjeta inteligente**

(30) Prioridad:

28.09.2011 FR 1158701

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.02.2015

(73) Titular/es:

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

(72) Inventor/es:

MORIN, NICOLAS y
GIRAUD, CHRISTOPHE

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Iniciación de ataques en componentes de tarjeta inteligente

Antecedentes de la invención

La invención se refiere al ámbito de los componentes seguros de tarjeta inteligente, o tarjeta de circuito integrado.

Para asegurar el funcionamiento de un componente de tarjeta inteligente, por ejemplo un microcontrolador, los constructores aplican pestillos de seguridad implantados en el código del componente.

Un ataque por inyección de fallo consiste en perturbar el componente para desviarlo de su comportamiento normal e intentar de este modo hacer “saltar” sus pestillos de seguridad. Tal ataque por inyección de fallo es por ejemplo realizada enviando un impulso luminoso al componente de tarjeta inteligente en un instante correspondiente a la ejecución de una instrucción determinada.

TOSHINORI FUKUNAGA ET ÁL.: "Practical Fault Attack on a Cryptographie LSI with ISO/IEC 18033-3 Block Ciphers" (FAULT DIAGNOSIS AND TOLERANCE IN CRYPTOGRAPHY (FDTC), 2009 WORKSHOP ON, IEEE, PISCATAWAY, NJ, USA, 6 septiembre 2009, páginas 84-92, ISBN: 978-1-4244-4972-9) describe un procedimiento de iniciación de ataques en un circuito criptográfico.

Para poner a prueba la seguridad de sus tarjetas inteligentes frente a tales ataques, un constructor de tarjetas inteligentes puede verse obligado a realizar él mismo ataques o a hacer que un tercero realice ataques, por ejemplo un organismo de certificación. La figura 1 representa un sistema de iniciación de ataques que se puede utilizar para realizar ataques por un constructor de tarjeta inteligente o un organismo de certificación.

El sistema 1 de la figura 1 comprende un ordenador 2, un lector 3 de tarjeta inteligente, una tarjeta inteligente 4, un osciloscopio 5 y un emisor láser 6.

El ordenador 2 está conectado al lector 3 por una conexión 7, por ejemplo un cable USB. El ordenador 2 puede enviar órdenes hacia el lector 3, por la conexión 7. El lector 3 es capaz de comunicarse con la tarjeta inteligente 4 por una conexión 8, por ejemplo conforme a la norma ISO7816. Cuando recibe una orden del ordenador 2, el lector 3 transmite la orden recibida a la tarjeta inteligente 4. La tarjeta inteligente 4 comprende componentes electrónicos, especialmente un microcontrolador 10 configurado para ejecutar instrucciones predeterminadas en respuesta a la recepción de una orden.

El ordenador 2 está asimismo conectado al osciloscopio 5 por una conexión 9, por ejemplo una conexión GPIB (por «*General Purpose Interface Bus*»), que permite al ordenador enviar mensajes al osciloscopio 5, especialmente un mensaje que solicita al osciloscopio 5 pasar de un estado desarmado a un estado armado. El osciloscopio 5 está conectado al emisor láser 6 por una conexión 11.

Se ha demostrado que las interacciones físicas de un módulo electrónico embarcado, por ejemplo un módulo de microcontrolador de tarjeta inteligente, con su entorno exterior son dependientes de las operaciones efectuadas por el módulo así como de los valores de las variables manipuladas por estas operaciones. Ejemplos de tales interacciones son el consumo de corriente del módulo (señal PA), la radiación electromagnética (señal EMA) o bien la señal de radiofrecuencia (señal RFA) que permite a una tarjeta sin contacto alimentarse y comunicarse.

De este modo, en la figura 1, se denomina SA la señal de análisis medida para analizar las operaciones efectuadas por el microcontrolador 10. La señal de análisis SA puede ser por ejemplo el consumo de corriente, la radiación electromagnética o la señal de radiofrecuencia de la tarjeta inteligente 4. La señal SA es proporcionada al osciloscopio 5.

Cuando está armado, el osciloscopio 5 está configurado para detectar un evento particular en la señal de análisis SA y para enviar una señal de iniciación D hacia el emisor láser 6 en respuesta a la detección del evento particular. El evento particular es por ejemplo un pico de amplitud de la señal SA, que corresponde a un pico de consumo de corriente durante la ejecución, por el microcontrolador 10, de una instrucción que implica la transmisión de una variable en un bus.

La figura 2 representa la iniciación de un ataque en el sistema 1 de la figura 1, en función del tiempo.

Inicialmente, el osciloscopio 5 está desarmado y no efectúa ningún análisis de la señal SA. Cada orden emitida por el ordenador 2 es transmitida a la tarjeta inteligente 4 por el lector 3. La tarjeta inteligente 4 ejecuta las instrucciones que corresponden a las órdenes recibidas.

A continuación, antes del envío de una orden de atacar, el ordenador 2 envía un mensaje M de armado al osciloscopio 5 (en la etapa E1). En respuesta a la recepción del mensaje M, el osciloscopio 5 se arma (etapa E2), lo

cual requiere una duración ΔT de aproximadamente 200 ms. Cuando está armado, el osciloscopio 5 analiza permanentemente la señal de análisis SA para detectar un evento particular en la señal de análisis SA (etapa E6).

Después de transcurrir la duración ΔT, el ordenador 2 envía una orden CMD al lector 3 (etapa E3) y el lector 3 transmite la orden CMD a la tarjeta inteligente 4. En respuesta a la recepción de la orden CMD, el microcontrolador 10 de la tarjeta inteligente 4 ejecuta instrucciones predeterminadas correspondientes a la orden CMD (etapa E5).

La orden CMD es una orden cuya ejecución comprende una instrucción de atacar. De este modo, durante la etapa E5, una instrucción determinada genera el evento particular en la señal de análisis SA (etapa E5a). Este evento es detectado por el osciloscopio 5 (etapa E6a) que envía entonces la señal de iniciación D al emisor láser 6.

En respuesta a la recepción de la señal de iniciación D, el emisor láser 6 envía un impulso luminoso a la tarjeta inteligente 4 (etapa E7).

El sistema de la figura 1 permite entonces, durante la ejecución de instrucciones en respuesta a la recepción de una orden, iniciar un ataque en un instante preciso que corresponde a la ejecución de una instrucción predeterminada. La orden atacada es determinada por el ordenador 2 que arma el osciloscopio 5 antes del envío de la orden enviando el mensaje M de armado.

El sistema 1 de la figura 1 presenta sin embargo inconvenientes. En efecto, el armado del osciloscopio (etapa E2) necesita un tiempo ΔT relativamente importante, típicamente del orden de 200 ms a comparar con aproximadamente 30 ms para la ejecución de una orden (etapa E5). El número de ataques que es posible iniciar en un tiempo determinado es por lo tanto limitado. Además, un osciloscopio 5 es un equipo costoso.

Por lo tanto existe una necesidad de una solución que permita iniciar ataques de manera más eficaz y menos costosa.

El sistema 1 de la figura 1 se ha descrito para facilitar la comprensión de la invención y de sus ventajas. Sin embargo, no se ha de deducir que el sistema 1 forma parte de la técnica.

Objeto y sumario de la invención

La presente invención propone un sistema de iniciación de ataques en un componente de tarjeta inteligente, que comprende un dispositivo informático, un lector de tarjeta inteligente y un dispositivo de análisis, estando el lector configurado para transmitir órdenes procedentes del dispositivo informático hacia una tarjeta inteligente, estando el dispositivo de análisis configurado para pasar de un estado desactivado a un estado activado en respuesta a la recepción de un mensaje de activación y, cuando está en su estado activado, para detectar un evento predeterminado en una señal de análisis procedente de una tarjeta inteligente y para enviar una señal de iniciación en respuesta a la detección de dicho evento.

Este sistema se caracteriza porque el dispositivo de análisis es un detector de motivo configurado para detectar dicho evento por digitalización de la señal de análisis sobre n bits, siendo n superior o igual a 3, y comparación de una porción de m muestras de la señal de análisis digitalizada, siendo m superior o igual a 3, con una señal de referencia.

Preferiblemente, el lector está configurado para enviar dicho mensaje de activación hacia dicho dispositivo de análisis en respuesta a la recepción de una orden determinada.

Correlativamente, la invención propone un procedimiento de iniciación de ataques en un componente de tarjeta inteligente, que comprende:

- una etapa de transmisión, por un lector de tarjeta inteligente, de órdenes procedentes de un dispositivo informático hacia una tarjeta inteligente,

- una etapa de paso, por un dispositivo de análisis, de un estado desactivado a un estado activado en respuesta a la recepción de un mensaje de activación,

- una etapa de detección, por el dispositivo de análisis en el estado activado, de un evento predeterminado en una señal de análisis procedente de una tarjeta inteligente, y

- una etapa de envío, por el dispositivo de análisis, de una señal de iniciación en respuesta a la detección de dicho evento.

Este procedimiento se caracteriza porque la etapa de detección de dicho evento comprende la digitalización de la señal de análisis sobre n bits, siendo n superior o igual a 3, y la comparación de una porción de m muestras de la señal de análisis digitalizada, siendo m superior o igual a 3, con una señal de referencia.

Preferiblemente, dicho mensaje de activación es enviado hacia dicho dispositivo de análisis por dicho lector en respuesta a la recepción de una orden determinada.

El sistema y el procedimiento de la invención permiten por lo tanto, durante la ejecución de instrucciones en respuesta a la recepción de una orden, iniciar un ataque en un instante preciso que corresponde a la ejecución de una instrucción predeterminada. La orden atacada es determinada por el instante de activación del dispositivo de análisis. El tiempo necesario para la transmisión del mensaje de activación es muy débil. Asimismo, el tiempo necesario para la activación del dispositivo de análisis es muy reducido en comparación con los largos procedimientos necesarios para el armado de un osciloscopio. De este modo, el tiempo necesario para la iniciación de un ataque es más reducido que en el caso de la figura 1. Por lo tanto es posible efectuar un mayor número de ataques en un tiempo determinado.

Si el dispositivo de análisis se activa demasiado pronto antes de la ejecución de la orden de atacar, es posible que detecte el evento particular en la señal de análisis sin que este evento corresponda a la instrucción de atacar. El envío del mensaje de activación por el lector de tarjeta durante la transmisión de la orden de atacar permite minimizar el desfase entre el comienzo de la ejecución de las instrucciones por la tarjeta inteligente y el comienzo del análisis efectuado por el dispositivo de análisis. En efecto, el lector es el elemento situado lo más próximo posible de la tarjeta inteligente y del dispositivo de análisis. Se minimiza de este modo el riesgo de falsa detección.

El lector puede estar configurado para memorizar una información que designa una orden en respuesta a un mensaje procedente del dispositivo informático, y para enviar dicho mensaje de activación hacia dicho dispositivo de análisis en respuesta a la recepción de la orden designada por la información memorizada.

La orden de atacar puede entonces ser designada fácilmente por el dispositivo informático enviando el mensaje hacia el lector.

En un modo de realización, dicha información es una variable que puede tomar un valor activado y un valor desactivado, estando el lector configurado para activar dicha variable en respuesta a la recepción del mensaje procedente del dispositivo informático y para enviar dicho mensaje de activación hacia dicho dispositivo de análisis en respuesta tras la recepción de una orden cuando la variable es activada.

La transmisión del mensaje del dispositivo informático hacia el lector y el cambio del valor de la variable solo necesita un tiempo muy reducido. Además, la memorización de la variable no necesita muchos recursos en el lector.

Ventajosamente, el dispositivo de análisis comprende un convertidor analógico/digital capaz de digitalizar la señal de análisis, una memoria intermedia configurada para memorizar una porción de la señal de análisis digitalizada, otra memoria que memoriza un motivo de referencia y una unidad de comparación configurada para comparar la porción de la señal de análisis memorizada por la memoria intermedia con dicho motivo de referencia.

La unidad de comparación puede estar configurada para determinar un grado de similitud entre la porción de la señal de análisis memorizada por la memoria intermedia y dicho motivo de referencia utilizando un algoritmo de intercorrelación. En este caso, el dispositivo de análisis puede comprender, además, otra una unidad de transformación configurada para efectuar una transformación de Fourrier de la señal de análisis digitalizada.

La memoria intermedia, dicha otra memoria y la unidad de comparación pueden estar incluidas en un circuito lógico programable o en un procesador de señales digital.

El tiempo necesario para la activación de tal detector de motivo es muy reducido, en comparación con el armado de un osciloscopio.

El sistema puede comprender, además, un emisor capaz de enviar un impulso luminoso hacia una tarjeta inteligente conectada al lector en respuesta a la recepción de la señal de iniciación.

La invención propone asimismo un lector de tarjeta inteligente configurado para transmitir órdenes procedentes de un dispositivo informático hacia una tarjeta inteligente, caracterizado porque está configurado para enviar un mensaje de activación hacia un dispositivo de análisis en respuesta a la recepción de una orden determinada.

La invención propone asimismo un dispositivo de análisis configurado para pasar de un estado desactivado a un estado activado en respuesta a la recepción de un mensaje de activación y, cuando está en su estado activado, para detectar un evento predeterminado en una señal de análisis procedente de una tarjeta inteligente y para enviar una señal de iniciación en respuesta a la detección de dicho evento, caracterizado porque está configurado para detectar dicho evento por digitalización de la señal de análisis y comparación de una porción de la señal de análisis digitalizada con una señal de referencia.

Breve descripción de los dibujos

Otras características y ventajas de la presente invención se pondrán de manifiesto a partir de la descripción realizada a continuación, con referencia a los dibujos anexos que ilustran un ejemplo de realización desprovisto de cualquier carácter limitativo. En las figuras:

- la figura 1 es un esquema que representa un sistema de iniciación de ataques,

- la figura 2 representa la iniciación de un ataque en el sistema de la figura 1, en función del tiempo,

- la figura 3 es un esquema que representa un sistema de iniciación de ataques conforme a la invención,

- la figura 4 representa la iniciación de un ataque en el sistema de la figura 3, en función del tiempo,

- la figura 5 es un esquema que representa el dispositivo de análisis del sistema de la figura 3 de manera más detallada, y

- la figura 6 es un gráfico que ilustra el funcionamiento del dispositivo de análisis de la figura 5.

Descripción detalladla de un modo de realización

La figura 3 representa un sistema 21 de iniciación de ataques que puede ser utilizado, por ejemplo por un constructor de tarjeta inteligente o un organismo de certificación, para realizar ataques. El sistema 21 de la figura 3 comprende un ordenador 22, un lector 23 de tarjeta inteligente, una tarjeta inteligente 24, un dispositivo de análisis 25 y un emisor láser 26.

El ordenador 22 está conectado al lector 23 por una conexión 27, por ejemplo un cable USB. El ordenador 22 puede enviar órdenes hacia el lector 33 por la conexión 27. El lector 23 es capaz de comunicarse con la tarjeta inteligente 24 por una conexión 28, por ejemplo conforme a la norma IS07816. Cuando recibe una orden del ordenador 22, el lector 23 transmite la orden recibida a la tarjeta inteligente 24.

La tarjeta inteligente 24 comprende componentes electrónicos, especialmente un microcontrolador 30 configurado para ejecutar instrucciones predeterminadas en respuesta a la recepción de una orden.

El lector 23 está asimismo conectado al dispositivo de análisis 25 por una conexión 29, por ejemplo una conexión GPIB (por «*General Purpose Interface Bus*»), que permite al lector 23 enviar mensajes al dispositivo de análisis 25, especialmente un mensaje que solicita al dispositivo de análisis 25 pasar de un estado inactivo a un estado activo. El dispositivo de análisis 25 está asimismo conectado al emisor láser 26 por una conexión 31.

Una señal de análisis SA es medida para analizar las operaciones efectuadas por el microcontrolador 30. La señal de análisis SA puede ser por ejemplo el consumo de corriente, la radiación electromagnética o la señal radiofrecuencia de la tarjeta inteligente 24. La señal SA es proporcionada al dispositivo de análisis 25.

Cuando está en su estado activo, el dispositivo de análisis 25 está configurado para detectar un evento particular en la señal de análisis SA y para enviar una señal de iniciación D hacia el emisor láser 26 en respuesta a la detección del evento particular. El evento particular es por ejemplo un pico de amplitud de la señal SA, correspondiente a un pico de consumo de corriente durante la ejecución, por el microcontrolador 30, de una instrucción que implica la transmisión de una variable en un bus.

Con este fin, el dispositivo de análisis 25 efectúa una digitalización de la señal de análisis SA y una comparación sobre la marcha de la señal de análisis digitalizada con una señal de referencia. Un ejemplo de realización del dispositivo de análisis 25 se describirá más adelante.

El lector 23 de tarjeta inteligente memoriza una variable, denominada en lo sucesivo «Enable_trigger», que puede adoptar los valores 0 y 1. Inicialmente, Enable_trigger vale 0. El lector 23 vigila permanentemente la recepción de mensajes procedentes del ordenador 22 por la conexión 27 y procesa los mensajes recibidos de la siguiente manera:

- Cuando el mensaje recibido es un mensaje de activación M1, el lector 23 cambia el valor de la variable Enable_trigger a 1.

- Cuando el mensaje recibido es una orden y Enable_trigger vale 0, el lector 23 transmite la orden recibida hacia la tarjeta inteligente 24.

- Cuando el mensaje recibido es una orden y Enable_trigger vale 1, el lector 23 transmite la orden recibida hacia la tarjeta inteligente 24, transmite un mensaje de activación M2 hacia el dispositivo de análisis 25 y cambia el valor de Enable_trigger a 0.

El lector 23 comprende por ejemplo un microcontrolador programado para aplicar el funcionamiento que se acaba de describir.

La figura 4 representa la iniciación de un ataque en el sistema 21 de la figura 3, en función del tiempo.

Inicialmente, el dispositivo de análisis 25 está inactivo y no efectúa ningún análisis de la señal SA. La variable Enable_trigger del lector 23 vale 0. Cada orden emitida por el ordenador 22 es transmitida a la tarjeta inteligente 24 por el lector 23. La tarjeta inteligente 24 ejecuta las instrucciones correspondientes a las órdenes recibidas.

A continuación, antes del envío de una orden de atacar, el ordenador 22 envía un mensaje de activación M1 al lector 23 (etapa S1). En respuesta a la recepción del mensaje M1, el lector 23 cambia el valor de la variable Enable_trigger a 1 (etapa S2). Enable_trigger es anotada como ET en la figura 4 para mayor claridad.

A continuación, el ordenador 22 envía una orden CMD al lector 23 (etapa S3). En respuesta a la recepción de la orden CMD, el lector 23 transmite la orden CMD a la tarjeta inteligente 24 (etapa S4). Además, como Enable_trigger vale 1, el lector 23 envía un mensaje de activación M2 al dispositivo de análisis (etapa S5) y cambia el valor de la variable Enable_trigger a 0 (etapa S6). En la figura 4, las etapas S4, S5 y S6 están representadas una tras otra, en este orden. Sin embargo, pueden ser ejecutadas en un orden diferente o en paralelo.

En respuesta a la recepción del mensaje de activación M2, el dispositivo de análisis 25 pasa a su estado activo. En este estado activo, el dispositivo de análisis 25 análisis permanentemente la señal de análisis SA para detectar un evento particular en la señal de análisis SA (etapa S8).

Paralelamente, en respuesta a la recepción de la orden CMD, el microcontrolador 30 de la tarjeta inteligente 24 ejecuta instrucciones predeterminadas que corresponden a la orden CMD (etapa S7).

La orden CMD es una orden cuya ejecución comprende una instrucción de atacar. De este modo, durante la etapa S7, una instrucción determinada genera el evento particular en la señal de análisis SA (etapa S7a). Este evento es detectado por el dispositivo de análisis (etapa S8a) que envía entonces la señal de iniciación D al emisor láser 26.

En respuesta a la recepción de la señal de iniciación D, el emisor láser 26 envía un impulso luminoso a la tarjeta inteligente 24 (etapa S9).

El sistema 21 de la figura 3 permite entonces, durante la ejecución de instrucciones en respuesta a la recepción de una orden, iniciar una ataque en un instante preciso correspondiente a la ejecución de una instrucción predeterminada. La orden atacada es determinada por el ordenador 22 que activa el dispositivo de análisis 25, mediante el lector 23, enviando el mensaje de activación M1 antes del envío de la orden CMD.

El tiempo necesario para la transmisión del mensaje de activación M1 (etapa S1), el cambio de Enable_trigger (etapa S2) y la transmisión del mensaje de activación M2 (etapa S5) es muy reducido, ya que se trata simplemente de transmitir mensajes y cambiar el valor de una variable. Asimismo, el tiempo necesario para la activación del dispositivo de análisis 25 es muy reducido en comparación con los largos procedimientos necesarios para el armado de un osciloscopio. De este modo, el tiempo necesario para la iniciación de un ataque en el sistema 23 de la figura 3 es más reducido que en el caso de la figura 1. Por lo tanto, es posible efectuar un mayor número de ataques en un tiempo determinado.

Si el dispositivo de análisis 25 se activa demasiado pronto antes de la ejecución de la orden de atacar, es posible que detecte el evento particular en la señal de análisis SA sin que este evento corresponda a la instrucción de atacar. El envío del mensaje de activación M2 por el lector 23 durante la transmisión de la orden CMD a la tarjeta inteligente 24 permite minimizar el desfase entre el comienzo de la ejecución de las instrucciones (etapa S7) y el comienzo del análisis efectuado por el dispositivo de análisis (etapa S8). En efecto, el lector 23 es el elemento situado más próximo a la tarjeta inteligente 24 y al dispositivo de análisis 25. Se minimiza de este modo el riesgo de falsa detección.

La figura 5 representa un ejemplo de realización del dispositivo de análisis 25 de la figura 3. El dispositivo de análisis 25 de la figura 5 es un detector de motivo que comprende un filtro 31, un convertidor analógico/digital 32 y un circuito de análisis 33.

El filtro 31 efectúa un procesamiento analógico sobre la señal de análisis SA, típicamente un filtrado de paso bajo. La señal filtrada es digitalizada en n bits por el convertidor analógico/digital 32. El número de bits n et superior o igual a 3, lo cual permite detectar motivos variados, por oposición a una simple detección binaria.

El circuito de análisis 33 comprende una memoria intermedia 34, otra memoria 35 y una unidad de comparación.

En el modo de realización representado, la unidad de comparación está compuesta por una unidad de intercorrelación 36 que efectúa un algoritmo de intercorrelación y por un detector de umbral 37 que permite medir la

similitud entre 2 curvas.

La memoria intermedia 34 memoriza sobre la marcha m muestras de n bits procedentes del convertidor analógico/digital 32, sobre el principio de «primero en llegar, primero en salir". De este modo, el contenido de la memoria intermedia 34 representa, en forma de m muestras de n bits, la parte más reciente de la señal de análisis SA. El número m de muestras es superior o igual a 3, lo cual permite comparar la forma de curvas durante una cierta duración.

La memoria 35 memoriza un motivo de m valores de n bits, correspondiente al envío que debe ser detectado en la señal de análisis SA.

La unidad de intercorrelación 36 determina un grado de similitud entre la curva memorizada en la memoria intermedia 34 y la curva memorizada en la otra memoria 35 utilizando un algoritmo de intercorrelación. A continuación, el grado de similitud se compara con un umbral S predeterminado en la unidad de detección de umbral 37. Si el grado de similitud es inferior al umbral S, se considera que la señal de análisis SA es diferente del motivo memorizado en la memoria 35 y la señal de iniciación D no es emitida. Sin embargo, si el grado de similitud es superior al umbral S, se considera que la señal de análisis SA corresponde al motivo memorizado en la memoria 35 y la señal de iniciación D es emitida.

En esta variante, el circuito de análisis 33 comprende preferiblemente una unidad de transformación no representada situada entre la salida del convertidor analógico/digital 32 y la entrada de las memorias 34 y 35. La unidad de transformación realiza una transformación de Fourrier de tipo FFT. Sabiendo que es más fácil aplicar un algoritmo de intercorrelación en el ámbito frecuencial que en el ámbito temporal, se facilita el trabajo de la unidad de comparación.

El funcionamiento del circuito de análisis 33 es activado en respuesta a la recepción del mensaje de activación M2 en la conexión 29, y desactivado después de la emisión de la señal de iniciación D.

El circuito de análisis 33 es realizado por ejemplo por un circuito lógico programable de tipo FPGA. En una variante, se trata de un procesador digital de señales (DSP) configurado para aplicar las funciones de la memoria intermedia 34, de la otra memoria 35 y de la unidad de comparación.

La figura 6 ilustra el funcionamiento del dispositivo de análisis 25 de la figura 5.

Durante una fase P1, la señal de análisis SA es digitalizada y una porción de la señal SA es memorizada en la memoria 35. Esta porción representa el motivo que hay que reconocer.

A continuación, durante una fase P2, la señal de análisis SA es digitalizada y comparada sobre la marcha con el motivo memorizado. Cuando el motivo es detectado, la señal de iniciación D es reconocida.

En el modo de realización descrito, la orden de atacar es determinada por el ordenador 22 que envía el mensaje de activación M1 justo antes de la orden de atacar. El lector 23 utiliza la variable Enable_trigger para memorizar que la próxima orden es la orden de atacar. Sin embargo, en una variante, la orden de atacar puede estar designada de otra manera. Por ejemplo, el ordenador 22 puede enviar un mensaje que contiene el identificador de una orden de atacar y el lector 23 memoriza este identificador. Esto permite enviar órdenes intermedias entre el mensaje y la orden de atacar.

El ordenador 22 es por ejemplo un ordenador personal. En una variante, puede tratarse de cualquier tipo de dispositivo informático capaz de enviar órdenes y un mensaje de activación hacia un lector de tarjeta.

REIVINDICACIONES

1. Sistema (21) de iniciación de ataques en un componente (30) de tarjeta inteligente (24), que comprende un dispositivo informático (22), un lector (23) de tarjeta inteligente y un dispositivo de análisis (25), estando el lector (23) configurado para transmitir órdenes procedentes del dispositivo informático (22) hacia una tarjeta inteligente (24), estando el dispositivo de análisis (25) configurado para pasar de un estado desactivado a un estado activado en respuesta a la recepción de un mensaje de activación (M2) y, cuando está en su estado activado, para detectar un evento predeterminado en una señal de análisis (SA) procedente de una tarjeta inteligente (24) y para enviar una señal de iniciación (D) en respuesta a la detección de dicho evento, caracterizado porque el dispositivo de análisis (25) es un detector de motivo configurado para detectar dicho evento por digitalización de la señal de análisis (SA) en n bits, siendo n superior o igual a 3, y comparación de una porción de m muestras de la señal de análisis digitalizada, siendo m superior o igual a 3, con una señal de referencia.

2. Sistema (21) de iniciación según la reivindicación 1, en el que el lector (23) está configurado para enviar dicho mensaje de activación (M2) hacia dicho dispositivo de análisis (25) en respuesta a la recepción de una orden (CMD) determinada.

3. Sistema (21) de iniciación de ataques según la reivindicación 2, en el que el lector (23) está configurado para memorizar una información que designa una orden en respuesta a un mensaje (M1) procedente del dispositivo informático (22), y para enviar dicho mensaje de activación (M2) hacia dicho dispositivo de análisis (25) en respuesta a la recepción de la orden (CMD) designada por la información memorizada.

4. Sistema (21) de iniciación de ataques según la reivindicación 3, en el que dicha información es una variable (ET) que puede adoptar un valor activado y un valor desactivado, estando el lector (23) configurado para activar dicha variable en respuesta a la recepción del mensaje (M1) procedente del dispositivo informático (22) y para enviar dicho mensaje de activación (M2) hacia dicho dispositivo de análisis (25) en respuesta a la recepción de una orden (CMD) cuando la variable (ET) está activada.

5. Sistema (21) de iniciación de ataques según una de las reivindicaciones 1 a 4, en el que el dispositivo de análisis (25) comprende un convertidor analógico/digital (32) capaz de digitalizar la señal de análisis (SA) sobre n bits, una memoria intermedia (34) configurada para memorizar una porción de m muestras de la señal de análisis digitalizada, una otra memoria (35) que memoriza un motivo de referencia y una unidad de comparación (36, 37) configurada para comparar la porción de la señal de análisis memorizada por la memoria intermedia (34) con dicho motivo de referencia.

6. Sistema (21) de iniciación de ataques según la reivindicación 5, en el que la unidad de comparación está configurada para determinar un grado de similitud entre la porción de la señal de análisis memorizada por la memoria intermedia (34) y dicho motivo de referencia utilizando un algoritmo de intercorrelación.

7. Sistema (21) de iniciación de ataques según la reivindicación 6, en el que el dispositivo de análisis comprende además otra una unidad de transformación configurada para efectuar una transformación de Fourrier de la señal de análisis digitalizada.

8. Sistema (21) de iniciación de ataques según una de las reivindicaciones 5 a 7, en el que la memoria intermedia (34), dicha otra memoria (35) y la unidad de comparación (36, 37) están incluidas en un circuito lógico programable (33).

9. Sistema (21) de iniciación de ataques según una de las reivindicaciones 5 a 7, en el que la memoria intermedia (34), dicha otra memoria (35) y la unidad de comparación (36, 37) están incluidas en un procesador de señales digital.

10. Sistema (21) de iniciación de ataques según una de las reivindicaciones 1 a 9, que comprende además otro un emisor (26) capaz de enviar un impulso luminoso hacia una tarjeta inteligente (24) conectada al lector (23) en respuesta a la recepción de la señal de iniciación (D).

11. Procedimiento de iniciación de ataques en un componente (30) de tarjeta inteligente (24), que comprende:

- una etapa de transmisión, por un lector (23) de tarjeta inteligente, de órdenes procedentes de un dispositivo informático (22) hacia una tarjeta inteligente (24),

- una etapa de paso, por un dispositivo de análisis (25), de un estado desactivado a un estado activado en respuesta a la recepción de un mensaje de activación (M2),

- una etapa (S8a) de detección, por el dispositivo de análisis (25) en el estado activado, de un evento predeterminado en una señal de análisis (SA) procedente de una tarjeta inteligente (24), y

- una etapa de envío, por el dispositivo de análisis (25), de una señal de iniciación (D) en respuesta a la detección de dicho evento;

caracterizado porque la etapa de detección de dicho evento comprende la digitalización de la señal de análisis sobre n bits, siendo n superior o igual a 3, y la comparación de una porción de m muestras de la señal de análisis digitalizada, siendo m superior o igual a 3, con una señal de referencia.

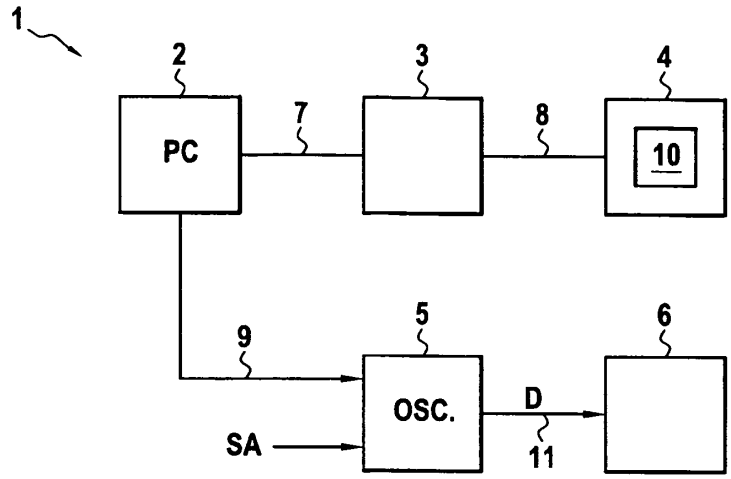

FIG.1

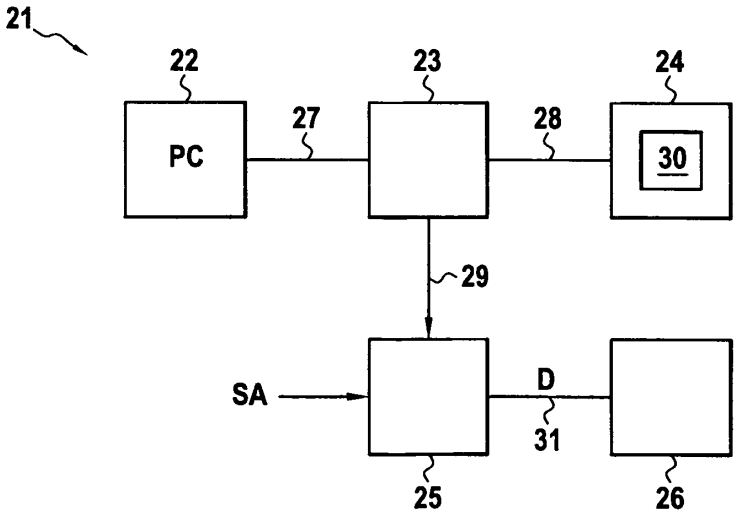

FIG.3

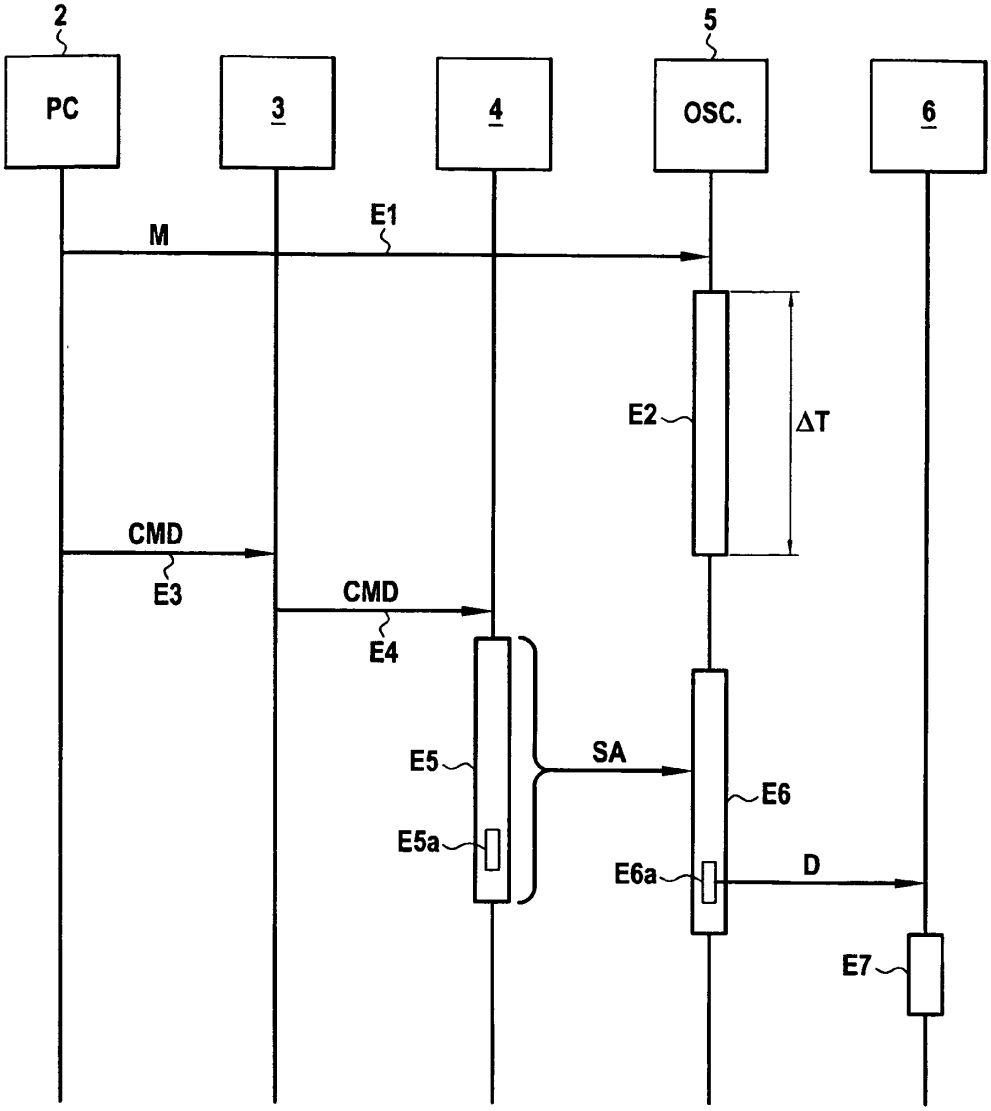

FIG.2

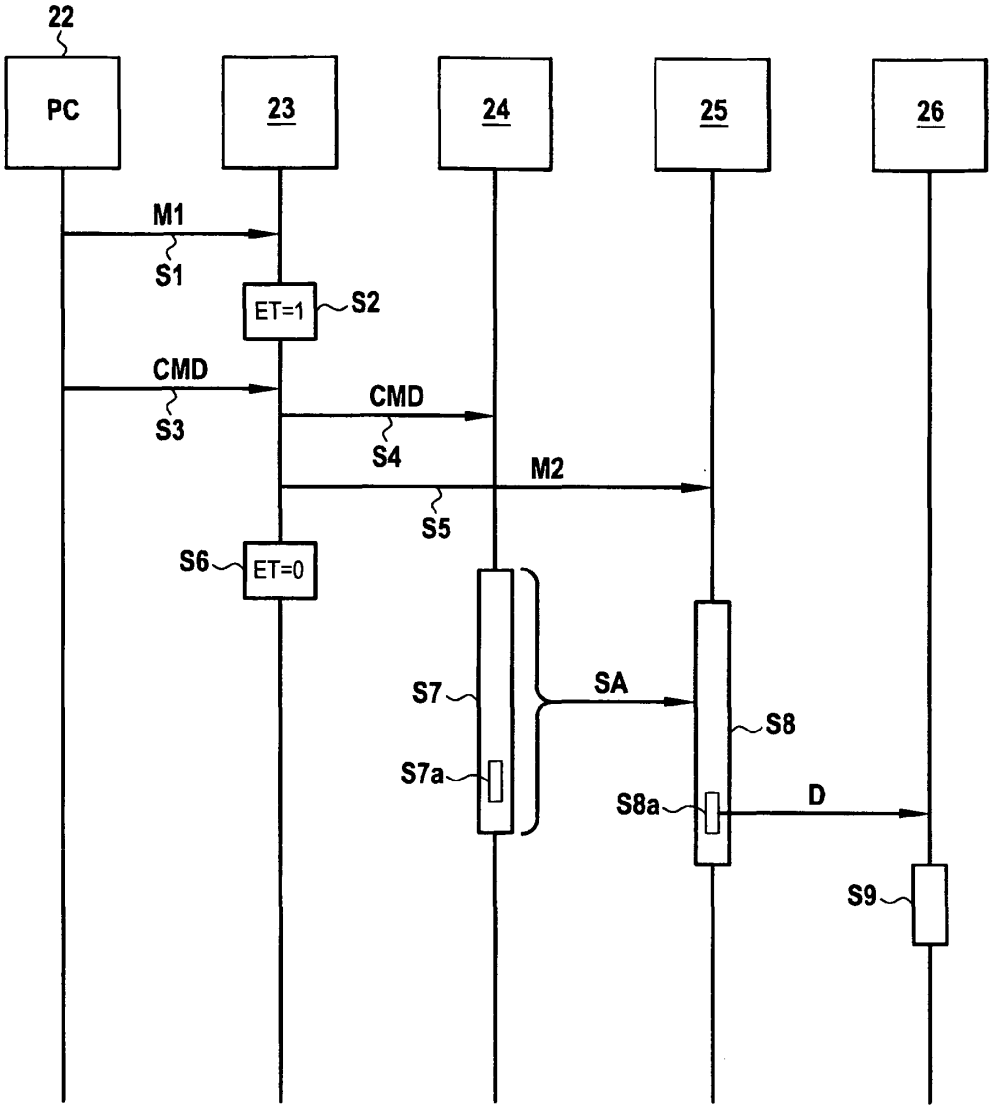
22
PC
23
24
25
26
M1
S1
ET=1
S2
CMD
S3
CMD
S4
M2
S5
S6
ET=0
S7
SA
S8
S7a
S8a
D
S9

FIG.4

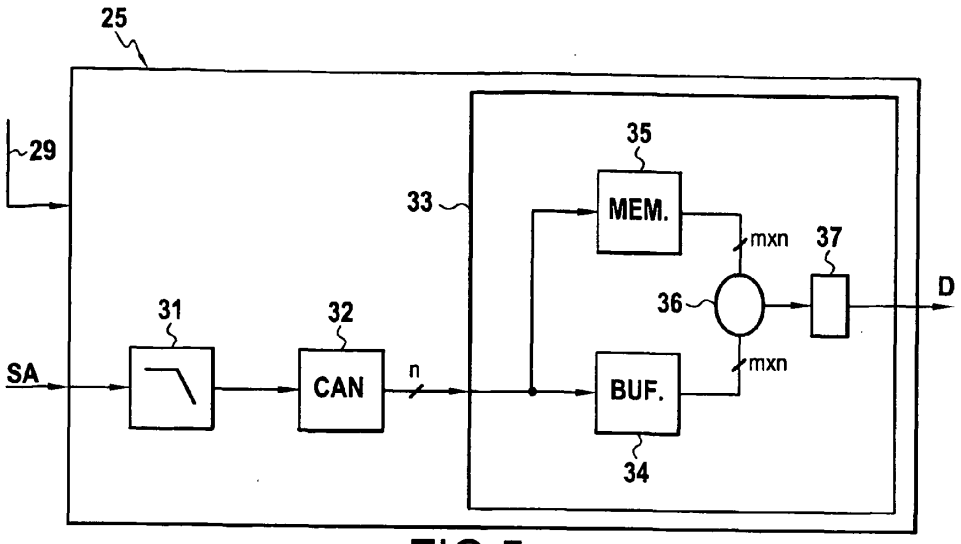
25
29
33
35
MEM.
mxn
37
D
36
31
32
SA
CAN
n
BUF.
mxn
34

FIG.5

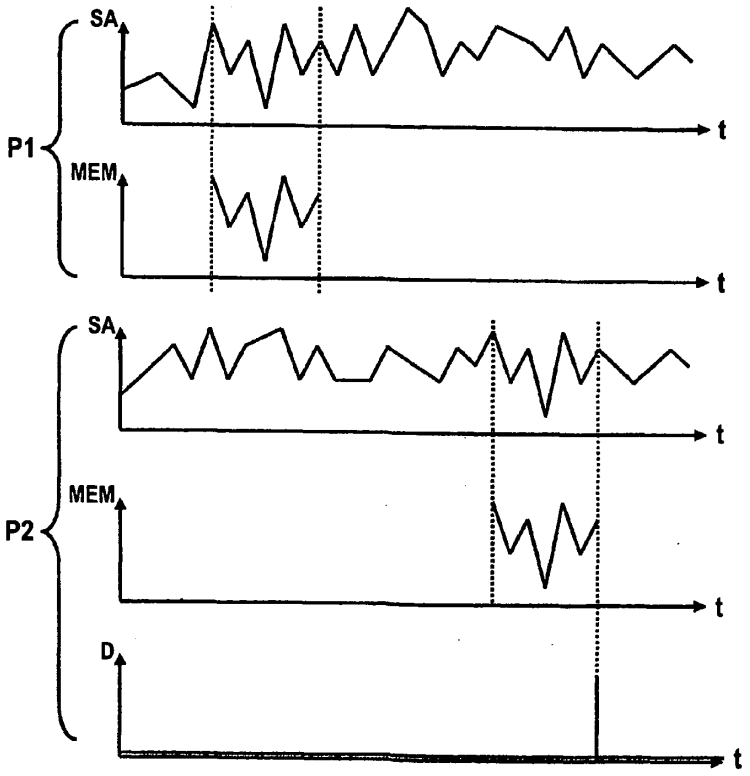
SA
t
P1
MEM
t
SA
t
MEM
P2
t
D
t

FIG.6