(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 619 635**

(51) Int. CI.:

G06F 21/57 (2013.01)
G06F 21/76 (2013.01)
G06F 21/31 (2013.01)
G06F 21/44 (2013.01)
H04L 9/08 (2006.01)
H04L 9/14 (2006.01)
H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.10.2013 PCT/EP2013/070889**

(87) Fecha y número de publicación internacional: **17.04.2014 WO2014056876**

(96) Fecha de presentación y número de la solicitud europea: **08.10.2013 E 13773769 (8)**

(97) Fecha y número de publicación de la concesión europea: **11.01.2017 EP 2907067**

(54) Título: **Método y sistema para personalización de chip de tarjeta inteligente**

(30) Prioridad:

11.10.2012 US 201261712274 P
11.10.2012 EP 12188097

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.06.2017

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

HAUTIER, ROAN;
MACCHETTI, MARCO y
PERRINE, JÉRÔME

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método y sistema para personalización de chip de tarjeta inteligente

Campo de la invención

[0001] La invención se refiere al dominio de la personalización de chip de tarjeta inteligente durante la que se introducen códigos secretos únicos y de aplicación.
En particular, los pasos de personalización se realizan bajo condiciones controladas para prevenir la clonación y reprogramación de tarjetas inteligentes en el campo.

Antecedentes técnicos

[0002] Los chips protegidos se usan en su mayoría en la fabricación de tarjetas inteligentes, módulos de seguridad, dispositivos de identificación y otros circuitos integrados usados en aplicaciones que requieren un alto nivel de seguridad.

[0003] El documento WO2010/130709A1 divulga un método para la autenticación de acceso a un chip protegido por un dispositivo de prueba.
Una vez el dispositivo de prueba se autentifica con el chip, es decir, se han realizado verificaciones exitosas por intercambios de datos de control entre el dispositivo de prueba y el chip, las diferentes pruebas operativas o simulaciones se realizan en funciones de hardware y software y/o programas implementadas en el chip.
El dispositivo de prueba puede comprender también funcionalidades de configuración o personalización del chip permitiendo, deshabilitando o programando características según los requisitos de aplicación previstos para el chip.
Según una implementación preferida, una ventaja de este método es minimizar la transferencia de datos entre el dispositivo de prueba y el chip protegido.
En respuesta a un desafío producido por el chip, el dispositivo de prueba envía un criptograma que será analizado y verificado por el chip antes de autorizar al dispositivo de prueba a ejecutar pruebas en dicho chip.

[0004] El documento EP1441313 se maneja en un método criptográfico asimétrico de protección de un chip de lógica electrónica por cable contra el fraude en transacciones entre el chip electrónico y una aplicación que incluye el cálculo del valor de autenticación de parámetros de entrada en el chip electrónico.
El método comprende los pasos de: producción por el chip de un número aleatorio específico a la transacción; envío a la aplicación de un primer parámetro calculado por la aplicación antes de la transacción, enlazado al número aleatorio por una relación matemática y almacenado en una memoria de datos del chip; cálculo por el chip de un segundo parámetro que constituye un valor de autentificación por medios de una función en serie, cuyos parámetros de entrada son al menos el número aleatorio específico para la transacción y una clave privada que pertenece a un par de claves asimétricas; envío del valor de autenticación a la aplicación, y verificación de dicho valor de autenticación mediante una función de verificación cuyos parámetros de entrada consisten exclusivamente en parámetros públicos que incluyen al menos la clave pública.

[0005] El documento EP1983466 describe el método y equipo de autentificación segura para el sistema en un chip (SoC).
El SoC puede permitir la autentificación de una entidad externa intentando ganar acceso a una función o sistema.
El SoC y una entidad externa autorizada pueden tener cada uno conocimientos de datos ocultos antes de un intento de autentificación y también pueden comunicar datos durante el proceso de autentificación.
Utilizar como datos, el SoC y una entidad externa puede ser capaz de generar la misma contraseña y conseguir acceso al sistema.
Las contraseñas pueden ser únicas en dos vías, por ejemplo: por operación y por dispositivo SoC.
Un generador de número aleatorio a bordo del SoC puede permitir las contraseñas para variar para cada iteración del proceso de autentificación.
Cada caso de un SoC tiene su propia palabra secreta que permite que las contraseñas sean únicas para cada dispositivo.

[0006] Después de la fabricación, los circuitos integrados de tarjeta inteligente o chips necesitan personalizarse para insertar secretos únicos y para cargar el código de aplicación en una vía muy segura para prevenir la clonación o reprogramación de tarjetas inteligentes hechas con estos chips.
Las soluciones tradicionales se basan en una estación informática dedicada que permite al personal instruido programar las tarjetas en la instalación de personalización (interna o externa).
Este método tiene muchos aspectos débiles y para superar estos aspectos se consideran los requisitos siguientes:

a) Hacer posible la personalización solo a nivel de oblea y extremadamente difícil para reactivar con medios físicos una vez la oblea se corte y los chip se empaqueten.

b) La activación de personalización no debería basarse solo en un secreto único o en el embalaje de software que puede poseer (y colar) el personal en la instalación de personalización.

c) Hacer imposible la repetición de secuencias de personalización para clonar chips destinados a ser implementados en tarjetas inteligentes.

d) Prevenir la ingeniería inversa completa del chip de tarjeta inteligente y así permitir que un atacante

reproduzca una personalización de chip.

Resumen de la invención

[0007] Los objetivos de la invención son cumplir mejor con los requisitos anteriormente mencionados sobre la personalización de chips de tarjeta inteligente y superar los inconvenientes de las soluciones de la técnica anterior.

[0008] El objetivo se consigue por un método de personalización de al menos un chip, destinado a ser integrado en una tarjeta inteligente, de forma que implica a un probador asociado a un dispositivo FPGA (matriz de puertas programable *in situ*) conectado al chip, el chip es parte de una oblea que induye una disposición de una pluralidad de chips, que comprende los pasos de:

- envío por el probador de un primer código secreto al dispositivo FPGA, dicho primer código secreto se almacena permanentemente en una memoria del probador,
- envío de por el dispositivo FPGA de un comando al chip para iniciar una secuencia de una activación de modo de prueba
- envío por medio del chip de una señal a un módulo de hardware desechable dispuesto en la oblea, dicho módulo de hardware retorna una respuesta que indica la presencia del chip en la oblea,
- generación y envío por medio del chip de un número aleatorio al dispositivo FPGA,
- encriptación por el dispositivo FPGA de un segundo código secreto usando un algoritmo de encriptación secreto parametrizado con el número aleatorio y el primer código secreto, obteniendo un primer criptograma,
- envío por el dispositivo FPGA del primer criptograma al chip,
- determinación por medio del chip de un segundo criptograma, realizando una función booleana sobre un resultado obtenido por la desencriptación del primer criptograma utilizando el inverso del algoritmo de encriptación secreto parametrizado con el número aleatorio y el primer código secreto,
- comparación por medio del chip del segundo criptograma con un resultado obtenido por la realización de la función booleana sobre el segundo código secreto temporalmente almacenado en el chip,
- si el segundo criptograma corresponde con el resultado obtenido por la realización de la función booleana sobre el segundo código secreto, permite a la secuencia de modo de prueba,
- el envío por medio del chip un mensaje de respuesta al dispositivo FPGA,
- realización por medio del dispositivo FPGA de la personalización del chip si el mensaje induye una respuesta positiva.

[0009] La invención se refiere además a un sistema configurado para la personalización de al menos un chip, destinado a ser integrado en una tarjeta inteligente, que comprende un probador asociado a un dispositivo FPGA (matriz de puertas programable *in situ*) conectado al chip, el chip es parte de una oblea que induye una disposición de una pluralidad de chips y un módulo de hardware desechable, caracterizado por el hecho de que:

- el probador se configura para enviar un primer código secreto al dispositivo FPGA, dicha primera cifra de seguridad se almacena permanentemente en una memoria del probador,
- el dispositivo FPGA se configura para enviar un comando al chip para iniciar una secuencia de una activación de modo de prueba, para encriptar un segundo código secreto usando un algoritmo de encriptación secreto parametrizado con un número aleatorio recibido desde el chip y el primer código seccreto, para obtener y enviar un primer criptograma al chip,
- el módulo de hardware desechable se configura para recibir una señal del chip y para devolver una respuesta que indica la presencia del chip en la oblea,
- el chip se configura para determinar un segundo criptograma por la realización de una función booleana sobre un resultado obtenido por desencriptación del primer criptograma utilizando el inverso del algoritmo de encriptación secreto parametrizado con el número aleatorio y el primer código secreto, y para comparar el segundo criptograma con un resultado calculado obtenido realizando la función booleana sobre el segundo código secreto temporalmente almacenado en el chip,
- el dispositivo FPGA está configurado además para ejecutar la personalización del chip solo si el modo del chip está permitido por una comparación exitosa entre el segundo criptograma y el resultado calculado.

[0010] Como de costumbre, la personalización es posible solo cuando el chip de tarjeta inteligente está en un estado especial, llamado "modo de prueba".
Por lo tanto, la solución se focaliza principalmente, pero no solo, en la prestación de la activación del modo de prueba muy seguro.

[0011] La protección de activación de modo de prueba se basa en diferentes características de seguridad, es decir:

- La utilización de un protocolo de desafío-respuesta anti-inverso basado en el método descrito en el documento WO2010/130709A1.
- La utilización de un módulo de hardware para verificar presencia del chip en la oblea.
  Este módulo de hardware se destruye después del corte de la oblea,
- La utilización de una plaza electrónica que incorpora un dispositivo FPGA, llamado "caja de oblea" que se integra mecánicamente y eléctricamente en el equipo de probador,
- La implementación de un generador de número aleatorio real (TRNG) en el chip de tarjeta inteligente que hace única estadísticamente la transacción de personalización.

Breve descripción de la figura

[0012] La invención se entenderá mejor con la siguiente descripción detallada, que se refiere a la figura adjunta dada como un ejemplo no limitativo.

[0013] La Figura 1 muestra un bloque esquemático que representa el sistema de la invención que comprende un probador asociado a un dispositivo FPGA conectado a al menos un chip de una oblea.
Antes de la personalización, el chip se monta en un modo de prueba por intercambios de datos de seguridad y verificaciones realizadas por el probador y el dispositivo FPGA.

Descripción detallada de la invención

[0014] El sistema ilustrado por la figura 1 comprende un probador T asociado a un dispositivo FPGA WB también llamado "caja de oblea" cuyo fichero de configuración es seguro con métodos conocidos para prevenir la clonación.
La activación de modo de prueba al igual que el proceso de personalización se realizan preferiblemente a nivel de oblea, es decir, los chips están dispuestos en una oblea usada para su fabricación.
Un módulo de hardware HM preferiblemente implementado en la oblea juega un papel de interfaz entre el dispositivo FPGA WB y los circuitos integrados de chips en la oblea W y está encargado de verificar la presencia de circuitos integrados de chip (s) en la oblea W después de la inicialización del modo de prueba.
Esta verificación previene manipulaciones o intenta modificar parámetros de personalización cuando un chip se corta fuera de la oblea o se integra en una tarjeta inteligente en servicio en el campo.
El módulo de hardware HM se destruye al final de proceso de personalización durante el corte de la oblea para separar todos los chips.
Además de estos medios de seguridad físicos, el software y los medios de seguridad de comunicación se usan también para proteger el proceso de personalización sensible.
La combinación de medios físicos y de software previene la personalización por terceras personas que poseen solo los programas software necesarios sin ningún enlace con un conjunto de circuitos de hardware físico desechable.

[0015] Al principio del proceso de personalización, el probador T se potencia al igual que el dispositivo FPGA y el chip IC.
El probador T lee y envía al dispositivo FPGA WB un primer código secreto S1 que se recupera de una memoria permanente del probador T.
Para comenzar introduciendo el chip en un modo de prueba, el dispositivo FPGA envía un comando C al chip IC que manda una señal s al módulo de hardware HM dispuesto en la oblea W.
El módulo de hardware HM devuelve una respuesta r al chip indicando su presencia en la oblea, es decir, no independiente o integrado en un dispositivo conectado al dispositivo FPGA WB.

[0016] En el caso del chip IC no recibe una respuesta r desde el módulo de hardware HM, la conexión con el módulo de hardware HM puede ser defectuosa o el chip IC se separa de la oblea W.
El probador T respectivamente al dispositivo FPGA WB para el procesamiento en comunicación con el módulo de hardware HM y se visualiza un mensaje de error.
Preferiblemente, un indicador de estado ST (chip en la oblea/chip fuera de la oblea) se puede proporcionar al dispositivo FPGA WB antes de la continuación de la activación de secuencia de modo de prueba.
Este indicador de estado ST se puede incluir en respuesta al comando de inicialización C.

[0017] Después de la comunicación exitosa con el módulo de hardware HM, el chip IC genera un número aleatorio R y lo reenvía al dispositivo FPGA WB.
Preferiblemente, el número aleatorio R es realmente aleatorio, es decir, producido con un generador de número aleatorio real de hardware (TRNG) para mejorar la singularidad estadística del resultado.

[0018] Hay dos métodos principales usados para generar números aleatorios: un primer método se basa en alguna medición de fenómeno físico (ruido en elementos semiconductores, por ejemplo) que se espera que sea aleatorio y luego compensa posibles perjuicios en el proceso de medición.
El segundo método usa algoritmos computacionales que pueden producir secuencias largas de resultados aparentemente aleatorios, que de hecho están completamente determinados por un valor inicial más corto, conocido como una semilla o clave.
El último tipo de generador se llama frecuentemente generador de número pseudo-aleatorio.
Un "generador de número pseudo-aleatorio" basado solamente en la computación determinista no se puede considerar como un generador de número aleatorio "real", ya que su emisión es previsible intrínsecamente.

[0019] El dispositivo FPGA WB encripta un segundo código secreto S2 usando un algoritmo de encriptación secreto E parametrizado con el número aleatorio R y el primer código secreto S1 para obtener un primer criptograma M1 = $_{ER,S1}$(S2) que se envía al chip IC.

[0020] El chip IC calcula un segundo criptograma M2 = F($E^{-1}_{R,S1}$(M1)) aplicando una función booleana F sobre un resultado obtenido desencriptando el primer criptograma recibido M1 con el inverso del algoritmo de encriptación

secreto E^{-1} parametrizado con el número aleatorio R y el primer código secreto S1.
Luego, este segundo criptograma M2 se compara por el chip IC con un resultado obtenido aplicando la función booleana F sobre el segundo código secreto S2 que se almacena temporalmente en el chip IC.
Si la comparación es exitosa, es decir, M2 = F(S2), la secuencia de modo de prueba se habilita de modo que el chip IC se prepara para ser personalizado.
De otro modo, los pasos precedentes que se inician por una nueva generación de número aleatorio R se puede repetir o el proceso se detiene debido a fallos de seguridad u otros defectos.
Cada intercambio de datos entre el dispositivo FPGA WB es único estadísticamente gracias al número aleatorio real R usado en la encriptación/desencriptación de algoritmo E para calcular los criptogramas M1 y M2.

[0021] La función booleana F puede ser preferiblemente una función unidireccional criptográfica tal como una función de control de tipo SHA256, por ejemplo, como se describe en el documento WO2010/130709A1.
Incluso se conoce la función F, es bastante imposible recuperar el valor original $E^{-1}_{R,S1}(M1)$ del criptograma resultante M2.

[0022] El dispositivo FPGA WB recibe el mensaje de respuesta RES como OK o KO desde el chip IC que indica que los pasos de personalización se pueden ejecutar o no.

[0023] Según una configuración preferida, el primer código secreto S1 y el segundo código secreto S2 constituyen partes de un código secreto global S. El primer código secreto S1 se almacena en una memoria permanente del probador T y en una memoria permanente del chip IC y se almacena en una memoria RAM de acceso aleatorio permanente del dispositivo FPGA WB.
El segundo código secreto S2 se almacena en una memoria permanente del dispositivo FPGA WB y se almacena en una memoria de acceso aleatorio permanente RAM del chip IC.
Se puede compartir el código secreto S por el almacenamiento de los códigos secretos S1 y S2 en las memorias respectivas del dispositivo FPGA y del chip IC al inicio del probador T cuando se inician las conexiones de los elementos del sistema.

[0024] Posteriormente, el dispositivo FPGA WB se configura para tener acceso a la memoria no volátil encriptada para cargar el código de aplicación en el chip IC durante el paso de personalización.
Esta memoria puede contener diferentes versiones del código de aplicación de modo que el probador T, respectivamente, el dispositivo FPGA WB selecciona una versión predefinida de un código de aplicación almacenado en la memoria del chip (IC).
Según una forma de realización, el código de aplicación se envía por medio del dispositivo FPGA WB al chip (IC) de forma segura por encriptación utilizando un algoritmo que depende de un número aleatorio real de una manera similar al proceso de activación de modo de prueba anteriormente descrito.

[0025] Según otra forma de realización, el dispositivo FPGA WB está mecánicamente y eléctricamente conectado al probador T, de tal manera que es inaccesible físicamente por los usuarios del probador T durante el paso de personalización del chip.
Además, los módulos electrónicos que componen el dispositivo FPGA WB están hechos a prueba de manipulaciones o resistentes a manipulaciones.

[0026] El dispositivo FPGA WB transmite al probador T información que comprende sus datos de estado actuales y datos del chip personalizado IC para fines de trazabilidad.

REIVINDICACIONES

1. Método para la personalización de al menos un chip (IC), destinado a ser integrado en una tarjeta inteligente, que comprende un probador (T) asociado a un dispositivo FPGA (WB) conectado al chip (IC), el chip (IC) es parte de una oblea (W) que incluye una disposición de una pluralidad de chips, que comprende los siguientes pasos:
envío por medio del probador (T) de un primer código secreto (S1) al dispositivo FPGA (WB), dicho primer código secreto (S1) se almacena permanentemente en una memoria del probador (T),
envío por medio del dispositivo FPGA (WB) de un comando (C) al chip (IC) para iniciar una secuencia de una activación de modo de prueba,
envío por medio del chip (IC) de una señal (s) a un módulo de hardware desechable (HM) dispuesto en la oblea, dicho módulo de hardware (HM) devuelve una respuesta (r) que indica la presencia del chip (IC) en la oblea (W),
generación y envío por medio el chip (IC) de un número aleatorio (R) al dispositivo FPGA (WB),
encriptación por medio del dispositivo FPGA (WB) de un segundo código secreto (S2) usando un algoritmo de encriptación secreto (E) parametrizado con el número aleatorio (R) y el primer código secreto (S1) y obtención de un primer criptograma $M1=E_{R,S1}(S2)$,
envío por medio del dispositivo FPGA (WB) del primer criptograma $M1=E_{R,S1}(S2)$ al chip (IC),
determinación por medio del chip (IC) de un segundo criptograma $M2 = F(E^{-1}{}_{R,S1}(M1))$ realizando una función booleana F mediante un resultado $E^{-1}{}_{R,S}(M1)$ obtenido desencriptando el primer criptograma (M1), utilizando el inverso (E^{-1}) del algoritmo de encriptación secreto (E) parametrizado con el número aleatorio (R) y el primer código secreto (S1),
comparación por medio del chip (IC) del segundo criptograma (M2) con un resultado F(S2) obtenido, transportando la función de booleana F al segundo código secreto (S2) temporalmente almacenado en el chip (IC),
si el segundo criptograma (M2) corresponde con el resultado F(S2) obtenido por el transporte de la función booleana F al segundo código secreto (S2), liberación del modo de prueba, envío por medio del chip (IC) de un mensaje de respuesta (Res) al dispositivo FPGA (WB),
realización, por medio del dispositivo FPGA (WB), de la personalización del chip (IC) si el mensaje (Res) incluye una respuesta positiva (OK).

2. Método, según la reivindicación 1, **caracterizado por el hecho de que** el primer código secreto (S1) y el segundo código secreto (S2) constituyen partes de un código secreto global (S), el primer código secreto (S1) se almacena una memoria permanente del probador (T) y en una memoria permanente del chip (IC) y se almacena en una memoria de acceso aleatorio no permanente del dispositivo FPGA (WB), el segundo código secreto (S2) se almacena en una memoria permanente del dispositivo FPGA (WB) y se almacena en una memoria de acceso aleatorio no permanente del chip (IC).

3. Método, según la reivindicación 1 o 2, **caracterizado por el hecho de que** la función booleana (F) es una función de control unidireccional criptográfica de tipo SHA256.

4. Método, según cualquiera de las reivindicaciones 1 a 3, **caracterizado por el hecho de que** el número aleatorio (R) es un número aleatorio real producido con un generador de número aleatorio real (TRNG) de hardware.

5. Método, según cualquiera de las reivindicaciones 1 a 4, **caracterizado por el hecho de que** un indicador de estado (ST) que indica la presencia del chip en la oblea se proporciona al dispositivo FPGA (WB) por el módulo de hardware (HM) antes de continuar la activación de secuencia de modo de prueba, dicho indicador de estado (ST) está incluido en una respuesta al comando de inicialización (C).

6. Método, según cualquiera de las reivindicaciones 1 a 5 **caracterizado por el hecho de que** el módulo de hardware (HM) se destruye al final del proceso de personalización durante el corte de la oblea para separar los chips.

7. Método, según cualquiera de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** la activación del modo de prueba se realiza en una pluralidad de chips (IC) en la oblea (W) en paralelo.

8. Sistema configurado para la personalización de al menos un chip (IC), destinado a ser integrado en una tarjeta inteligente, que comprende un probador (T) asociado a un dispositivo FPGA (matriz de puertas programable *in situ*) (WB) conectado al chip (IC), el chip (IC) es parte de una oblea (W) que incluye una disposición de una pluralidad de chips y un módulo de hardware desechable (HM), **caracterizado por el hecho de que**:
- el probador (T) se configura para enviar un primer código secreto (S1) al dispositivo FPGA (WB), dicho primer código secreto (S1) se almacena permanentemente en una memoria del probador (T),
- el dispositivo FPGA (WB) se configura para enviar un comando (C) al chip que inicia una secuencia de una activación de modo de prueba, para encriptar un segundo código secreto (S2), usando un algoritmo de encriptación secreto (E) parametrizado con un número aleatorio (R) recibido del chip (IC) y el primer código secreto (S1), para obtener un primer criptograma (M1) y enviarlo al chip (IC),
- el módulo de hardware desechable (HM) se configura para recibir una señal (s) del chip (IC) y para devolver una respuesta (r) que indica la presencia del chip (IC) en la oblea (W),
- el chip (IC) se configura para determinar un segundo criptograma (M2) por el transporte de una función

booleana (F) mediante un resultado obtenido por desencriptación del primer criptograma (M1) utilizando el inverso del algoritmo de encriptación secreto (E^{-1}) parametrizado con el número aleatorio (R) y el primer código secreto (S1) y para comparar el segundo criptograma (M2) con un resultado calculado F(S2) obtenido realizando la función booleana (F) mediante el segundo código secreto (S2) temporalmente almacenado en el chip (IC),

- posteriormente, el dispositivo FPGA (WB) está configurado para ejecutar la personalización del chip (IC) solo si el modo de prueba del chip (IC) se libera por una comparación exitosa entre el segundo criptograma (M2) y el resultado calculado F(S2).

9. Sistema, según la reivindicación 8, **caracterizado por el hecho de que** el dispositivo FPGA (WB) se configura posteriormente para acceder a la memoria no volátil encriptada del chip (IC) y para cargar el código de aplicación en el chip IC durante el paso de personalización.

10. Sistema, según la reivindicación 9, **caracterizado por el hecho de que** el dispositivo FPGA (WB) se configura para seleccionar una versión predefinida de un código de aplicación cargado en la memoria no volátil encriptada bajo una pluralidad de versiones del código de aplicación almacenado en dicha memoria del dispositivo FPGA (WB).

11. Sistema, según la reivindicación 9, **caracterizado por el hecho de que** el dispositivo FPGA (WB) se configura para enviar el código de aplicación al chip (IC) de modo seguro por encriptación utilizando un algoritmo que depende de un número aleatorio real (R) producido previamente por el chip (IC).

12. Sistema, según la reivindicación 8 a 11, **caracterizado por el hecho de que** el dispositivo FPGA (WB) dispone de módulos a prueba de manipulaciones o resistentes a manipulaciones y conectados mecánicamente y eléctricamente al probador (T), de tal manera que sea inaccesible físicamente para los usuarios del probador (T) durante el paso de personalización del chip (IC).

13. Sistema, según cualquiera de las reivindicaciones 8 a 12, **caracterizado por el hecho de que** el dispositivo FPGA (WB) se configura para transmitir al probador (T) información que comprende los datos de estado actual de dicho dispositivo FPGA (WB) y los datos de historial del chip personalizado (IC) para fines de trazabilidad.

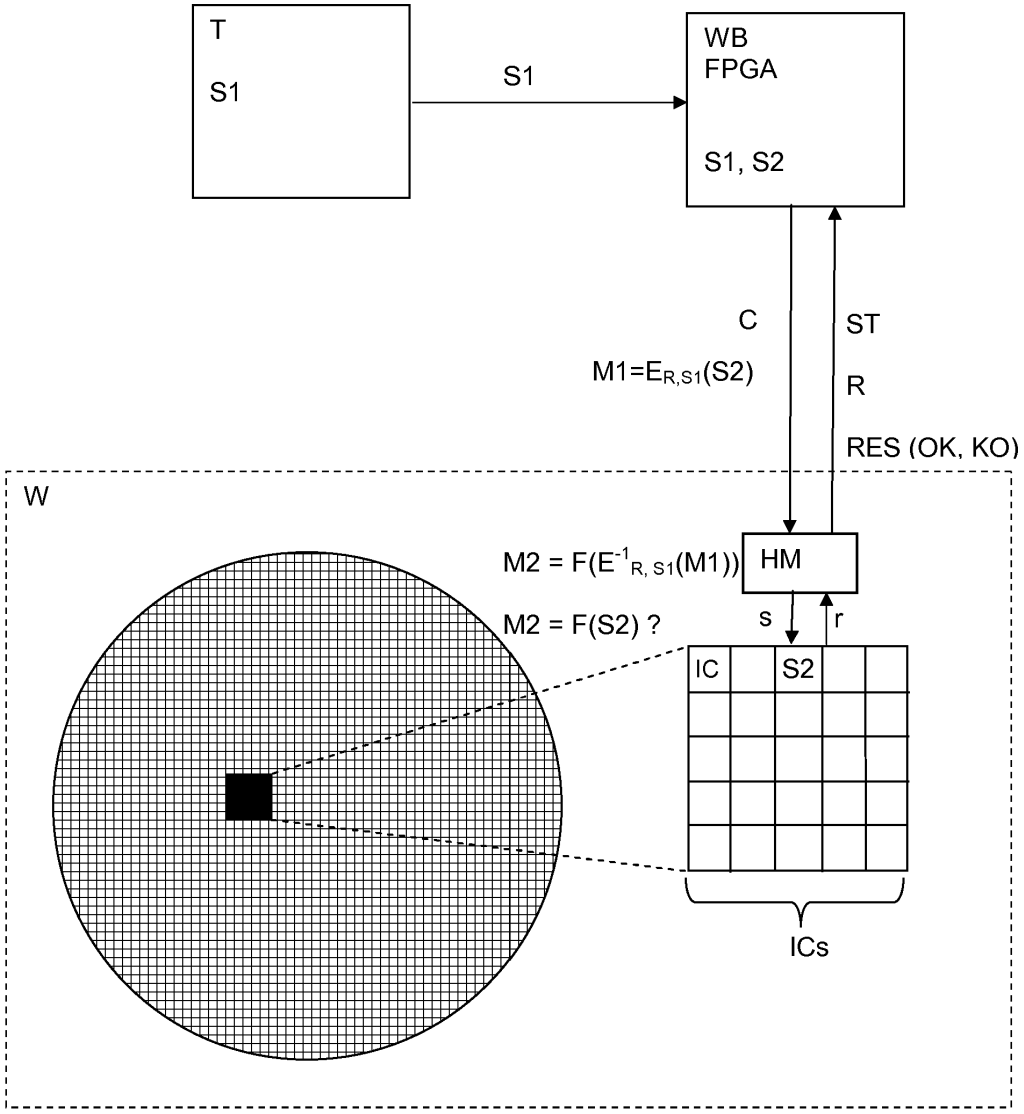
T
S1
S1
WB
FPGA
S1, S2
C
M1=E_R,S1(S2)
ST
R
RES (OK, KO)
W
M2 = F(E^-1_R, S1(M1))
HM
M2 = F(S2) ?
s
r
IC
S2
ICs

Fig. 1