(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 362 462**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08737723 .0**
(96) Fecha de presentación : **04.04.2008**
(97) Número de publicación de la solicitud: **2145448**
(97) Fecha de publicación de la solicitud: **20.01.2010**

(54) Título: **Activación controlada de función.**

(30) Prioridad: **12.04.2007 EP 07106038**

(45) Fecha de publicación de la mención BOPI:
06.07.2011

(45) Fecha de la publicación del folleto de la patente:
06.07.2011

(73) Titular/es: **INTRINSIC ID B.V.**
High Tech Campus 9
5656 AE Eindhoven, NL

(72) Inventor/es: **Talstra, Johan, C.;**
Tuyls, Pim, T. y
Schobben, Daniel, W., E.

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Activación controlada de función

Campo de la invención

La invención se refiere a activación controlada de al menos una función en un producto o un componente tal como un chip, un FPGA o un módulo de software.

Antecedentes de la invención

Productos tales como televisores, teléfonos móviles, reproductores DVD, ordenadores, ordenadores personales portátiles y otros aparatos electrónicos, así como también los programas de ordenador para tales productos, implementan una gran diversidad de características o funciones. Estas funciones se denominan habitualmente bloques de propiedad intelectual (IP) y son proporcionados por proveedores de IP, una o más compañías diferentes u otras entidades. Los bloques de IP pueden ser proporcionados, por ejemplo, como parte de diseños de chips, corrientes de bits para matrices de puerta programable en campo (FPGAs) o componentes de software.

Puesto que estos bloques de IP se encuentran con frecuencia disponibles sobre la base de un royalty por producto, es deseable controlar la activación de estos bloques de IP. Es decir, un bloque de IP no deberá estar en operación en un producto a menos que se haya informado de este hecho a, y opcionalmente sea autorizado por, un proveedor de IP.

Soluciones conocidas en este campo incluyen informar de un identificador único asociado al producto o bloque de IP, a un servidor remoto, con lo que el servidor devuelve un código de autorización asociado al identificador único.

Con preferencia, el código de autorización está diseñado de tal manera que solamente con un código de autorización correcto, la funcionalidad del bloque de IP puede ser activada. La activación en este contexto se implementa con frecuencia comparando el código de autorización con un código predefinido disponible en el bloque de IP. Si los códigos no se emparejan, la función no se habilita. El código de autorización puede ser también utilizado como clave para desbloquear o descodificar todo o parte del bloque de IP, por ejemplo como clave de descodificación para descodificar una corriente de datos que ha de ser cargada en una FPGA para provocar que la FPGA proporcione la función en cuestión.

Por ejemplo, cada plataforma Xilinx Spartan™-3A está dotada de un número de serie único, mencionado como “ADN de Dispositivo”. Los datos de configuración comprenden un valor de autenticación que corresponde con el ADN de Dispositivo de un espécimen particular. Cada espécimen está equipado con un módulo que verifica si el ADN de Dispositivo de la plataforma se empareja con el valor de autenticación, y habilita toda o parte de la funcionalidad del módulo solamente si existe tal emparejamiento, es decir, si está presente el dato de configuración correcto.

El código de autorización puede ser utilizado también como clave necesaria para procesar la entrada proporcionada en el bloque de IP, por ejemplo como clave de descodificación para que el contenido audiovisual sea descodificado por el bloque de IP, o para autenticar el producto en un servidor remoto con el que se debe intercambiar el dato.

El documento WO 2006/053304, incorporado en la presente memoria por referencia, divulga un procedimiento de determinación de una clave a partir de una función físicamente no clonable (PUF) prevista en tal dispositivo. Esto incluye aplicar datos de control de error a la respuesta de la PUF. La clave puede ser utilizada entonces, por ejemplo, para permitir que el dispositivo descifre datos tales como el contenido audiovisual codificado, o se autentifique a sí mismo respecto a otras partes.

Otra alternativa para obtener una clave a partir de una PUF ha sido descrita por B. Skoric, P. Tuyls y W. Ophey, “Extracción robusta de clave a partir de Funciones Físicas No Clonables”, Criptografía Aplicada y Seguridad de Red ACNS 2005, LNCS 3531, pp. 407-422 (2005). Se extrae una clave de una respuesta de PUF aplicando determinados datos auxiliares a la respuesta cruda.

Un problema de este campo es el de la clonación. Un bloque de IP o incluso un dispositivo completo, puede ser copiado en su totalidad, es decir, incluyendo el identificador único asociado. El bloque de IP del clon puede ser activado ahora utilizando el mismo código de autorización que el bloque de IP del original. El clon no tiene así necesidad de ser notificado al servidor remoto, causando una sub-notificación de bloques de IP activados y una pérdida asociada de royalties.

Para proteger contra la clonación, se encuentran disponibles diversas soluciones que proporcionan identificadores supuestamente no clonables. Por ejemplo, el documento WO 2006/071380, incorporado en la presente memoria por referencia, divulga un dispositivo configurable en campo, tal como una FPGA, que soporta configuración de campo segura sin utilizar ningún almacenamiento volátil o no-volátil para claves criptográficas en el dispositivo. Este dispositivo está dotado de una función físicamente no clonable o PUF que, dada una proposición, proporciona una salida que es única para cada espécimen particular del dispositivo. Sin embargo, una PUF particular no puede ser

clonada o reproducida en otro dispositivo. Para asegurar que se genera la misma salida, se necesita aplicar determinados datos de corrección de error a una determinada respuesta. Esto hace que sea posible extraer los datos de configuración desde la salida de una PUF. Solamente un espécimen particular puede entonces reconstruir con éxito los datos de configuración.

Generalmente hablando, estas alternativas proporcionan protección contra la copia no autorizada vinculando el bloque de IP a un espécimen particular de un producto por medio de un elemento único extraído de la PUF. Una copia del bloque de IP no podrá operar sobre un espécimen diferente debido a que la PUF de ese espécimen diferirá de la PUF del espécimen original, lo que provocará que falle la reconstrucción de los datos de configuración. Esto puede conducir a un valor o clave de autenticación erróneo.

Estas soluciones tienen en común el hecho de que, en algún punto, el identificador necesita ser leído y suministrado al servidor remoto para recibir el correspondiente código de autorización. Durante ese proceso, tanto el identificador como el código de autorización pueden ser observados y registrados. A continuación se puede producir aún un clon, por ejemplo dotando al clon de un simple chip que reproduzca el identificador observado. Este chip reemplaza entonces la memoria u otro elemento que proporcione originalmente el identificador.

Se pueden adoptar medidas para impedir el espionaje en el proceso de activación, pero éstas son complejas y pueden rebasar las capacidades de muchos dispositivos. El documento WO 2006/071380 mencionado anteriormente utiliza codificación de clave pública, para transferir con seguridad el identificador, o recomienda el uso de un procedimiento de inscripción separado en un entorno de confianza.

Además, los inventores han descubierto que lo anterior supone implícitamente una confianza absoluta en la entidad que programa o carga estos datos auxiliares en el componente o producto en cuestión. En muchos casos, esta entidad será una tercera parte fabricante que fabrica los productos o los componentes intermedios. Esta entidad deberá notificar al (a los) proveedor(es) de IP cuáles y cuántos productos han sido fabricados por la misma, de modo que pueda ser cargado el derecho de royalty respecto a los bloques de IP que haya utilizado.

Sin embargo, un fabricante puede fabricar más utilizando simplemente las mismas instalaciones que utilizó para los productos “oficiales”. Estos productos extra tienen, por supuesto, su propia PUF única, pero el fabricante está capacitado para dotarlos de los datos auxiliares correctos, lo que provocará que los bloques de IP que se basen en la PUF, funcionen como si estuvieran instalados en los originales. El fabricante tiene que saber cómo proporcionar los datos auxiliares a menos que no pueda fabricar los productos oficiales. Esto hace que sea posible para un fabricante hacer pasar estos productos extra, no autorizados, como originales. Ahora es también posible sub-notificar el número de productos fabricados, lo que significa que el proveedor de IP recibe royalties más bajos de lo que le corresponden.

Así, existe una necesidad de un procedimiento de activación controlada de una función que impida la activación de dispositivos clonados.

Sumario de la invención

La invención proporciona un procedimiento de activación controlada de al menos una función en un producto o componente en una posición remota, cuya activación requiere que se encuentre disponible en el producto o componente un elemento de datos de activación correcta, caracterizado por recibir una o más salidas ruidosas de un elemento no clonable asociado al componente desde la posición remota, y proporcionar datos auxiliares a la posición remota, cuyos datos auxiliares transforman la una o más señales ruidosas en un valor simple que se corresponde con el elemento de datos de activación correcta.

Los componentes no clonables con salidas ruidosas son conocidos en sí mismos. Un nombre de tales componentes es el de Funciones Físicas Aleatorias (No Clonables) o PUFs. Los datos auxiliares denominados de ese modo proporcionan redundancia para transformar esas respuestas ruidosas en un valor simple que puede ser elegido arbitrariamente. Es decir, la misma respuesta ruidosa puede ser transformada en diferentes valores simples mediante una elección apropiada de los datos auxiliares.

La invención propone computar estos datos auxiliares en una posición que es remota respecto a donde está situado el producto o componente que debe ser activado. Para activar la función, debe estar disponible un elemento de activación correcto. Los datos auxiliares transforman la una o más salidas ruidosas en un valor simple que corresponde con el elemento de datos de activación correcta. Los datos auxiliares se transmiten hasta la posición remota donde reside el producto o componente. Esto permite que el producto o componente extraiga el elemento de datos de activación correcta.

Sorprendentemente, este uso impide la activación de dispositivos clonados. El componente no clonable, por definición, no puede ser clonado. Un segundo componente no puede ser activado utilizando los datos auxiliares recibidos para una primera respuesta, puesto que los datos auxiliares únicamente están vinculados a la respuesta ruidosa producida por la PUF para el primer componente (y transforma esa respuesta en un identificador único y robusto). Aplicar esos datos auxiliares a una respuesta ruidosa producida por la PUF para el segundo componente, no dará como resultado la correcta activación del elemento de datos. Debido a la necesidad de incluir una entidad

remota para la activación, según propone la invención, el proceso de activación no puede ser eludido.

Obsérvese que “un elemento de datos de activación” puede comprender múltiples bits o bytes de datos. De manera similar, el “valor simple” que antecede consistirá típicamente en múltiples bits o bytes de datos.

El documento WO 2006/071380 mencionado anteriormente, divulga un dispositivo que está dotado de una función físicamente no clonable o PUF que, dado un supuesto, proporciona una salida que es única para cada espécimen particular del dispositivo. Para asegurar que se produce la misma salida, se necesita aplicar determinados datos de corrección de error a una respuesta determinada. La salida se suministra a continuación a un servidor remoto, el cual devuelve un código de autorización que ha sido blindado utilizando la salida, por ejemplo como resultado de una operación XOR que combina la salida y el código de autorización.

Una diferencia clave con la presente invención consiste en que, en este sistema, la salida según se envía al servidor *ha sido estabilizada* y por lo tanto no es ruidosa. Esto requiere que el dispositivo debe medir y estabilizar la respuesta durante la inscripción, lo que necesita un tiempo que puede no estar disponible, especialmente cuando la inscripción tiene lugar durante la producción. La invención, por el contrario, desplaza la estabilización, la computación de datos auxiliares, al lado del servidor.

Además, la alternativa del documento WO 2006/071380 necesita dos etapas: la primera, estabilizar la respuesta ruidosa, y la segunda utilizar la salida estabilizada para suministrar de forma segura un código de autorización. La presente invención *realiza ambas en una única etapa integrada*. Los datos auxiliares se computan de tal manera que se transforma la una o más salidas en un valor simple que corresponde con el elemento de datos de activación correcta. Existe por tanto una relación entre los datos auxiliares y el código de activación, cuya relación no se encuentra en la alternativa del documento WO 2006/071380.

Esta relación, entre otras cosas, reduce la cantidad de datos que se necesita almacenar. La presente invención solamente necesita almacenar los datos auxiliares. La aplicación de los datos auxiliares a la respuesta ruidosa produce el elemento de datos de activación. La alternativa del documento WO 2006/071380 necesita almacenar tanto los datos de corrección de error (para estabilizar la respuesta ruidosa) como el código de autorización blindado.

Una realización de la presente invención comprende transmitir el elemento de autenticación para establecer autenticidad de los datos auxiliares en la posición remota. Esto asegura que ningún tercero puede proporcionar datos auxiliares que habiliten la funcionalidad del componente. El componente debe estar configurado en esta realización para emplear solamente los datos auxiliares si la autenticidad de los datos auxiliares puede ser verificada utilizando el elemento de autenticación. Por ejemplo, el elemento de autenticación puede ser una signatura digital separada o un código de autenticación de mensaje. Alternativamente, los datos auxiliares pueden ser codificados con una clave, por ejemplo utilizando una operación tal como XOR o codificación de clave pública.

En una variante de esta realización, el elemento de autenticación se obtiene mediante la transmisión de los datos auxiliares a una tercera parte, y la recepción del elemento de autenticación en respuesta desde esa tercera parte. Esta realización asegura que la parte que habilita la funcionalidad no puede suministrar datos auxiliares sin que la tercera parte, típicamente el proveedor del componente en cuestión, la conozca. Dos opciones de implementación posibles consisten en un cuadro negro en la parte de confianza, y un servidor remoto en el proveedor de IP contactado en tiempo real por la parte de confianza.

En otra variante, los datos auxiliares son codificados con anterioridad a transmitirlos a la tercera parte. Con la codificación de los datos auxiliares, se asegura que la tercera parte no obtiene acceso a los propios datos auxiliares. Esto le evita tener que aprender cómo construir datos auxiliares para respuestas particulares. A continuación, se utiliza preferentemente una firma ciega para firmar los datos auxiliares.

Una realización adicional comprende recibir un elemento de autenticación remota desde la posición remota, y proporcionar los datos auxiliares solamente si los datos auxiliares pueden ser autenticados con éxito utilizando el elemento de autenticación remota. Esto ayuda a proteger la comunicación contra falsificaciones e intentos de sobrecargar el sistema enviando datos elegidos aleatoriamente.

En una realización adicional, los datos auxiliares son transmitidos a una segunda posición remota diferente de la posición remota desde la que se ha recibido la una o más respuestas. En esta realización es más difícil burlar el sistema. Ahora tienen que colaborar dos partes.

En una realización adicional, la una o más salidas ruidosas recibidas se comparan frente a la pluralidad de salidas ruidosas previamente recibidas, y los datos auxiliares se proporcionan solamente si la una o más salidas ruidosas no han sido recibidas previamente. Esto proporciona seguridad frente a ataques repetidos en los que se proporcionan las mismas salidas ruidosas múltiples veces. La comparación puede ser una comparación con pérdidas, es decir las salidas ruidosas recibidas pueden diferir una pequeña cantidad con las salidas ruidosas previamente recibidas. Si se estima que el emparejamiento es “suficientemente bueno” (por ejemplo, el 90% de los bits de las salidas se corresponden), la comparación se considera positiva.

La invención proporciona adicionalmente un sistema que implementa el procedimiento.

Breve descripción de las figuras

Estos y otros aspectos de la invención se pondrán de manifiesto a partir de, y podrán ser aclarados con referencia a, las realizaciones ilustrativas que se muestran en los dibujos, en los que:

La Figura 1 muestra esquemáticamente un sistema para la activación controlada de al menos una función en un producto o componente en una posición remota;

la Figura 2 muestra esquemáticamente una primera realización de este sistema;

la Figura 3 muestra esquemáticamente una segunda realización de este sistema, y

la Figura 4 muestra esquemáticamente una tercera realización de este sistema.

En las Figuras, los mismos números de referencia indican características similares o correspondientes. Algunas de las características indicadas en los dibujos están típicamente implementadas en software, y como tales representan entidades de software, tal como módulos u objetos de software.

Descripción detallada de realizaciones preferidas

La Figura 1 muestra esquemáticamente un sistema 110 para la activación controlada de al menos una función 142 en un producto o componente 140 en una posición remota 130. La activación del producto o componente 140, en este caso un microchip, requiere que un elemento de datos de activación correcta se encuentre disponible en el producto o componente 140. El producto o componente 140 es en este caso un microchip, pero podría ser igualmente cualquier clase de producto o componente. Algunos ejemplos son los teléfonos móviles, ordenadores, ordenadores personales portátiles, relojes, sensores, máquinas, aviones, placas de circuito e incluso software de ordenador. El único requisito de la presente invención consiste en que el producto o componente 140 tenga una función que necesite ser activada de una manera controlada.

La posición remota 130 será, con preferencia, una planta de fabricación o una fábrica en la que el producto o componente se ensambla o se produce. El término “remoto” en este contexto debe ser entendido como indicativo de que el sistema 110 y la posición 130 no son uno solo ni lo mismo. En una realización, la planta o la fábrica está situada en la República Popular de China y el sistema 110 está situado en el Reino de Holanda. En otra realización, el sistema se implementa como cuadro negro para ser instalado en algún lugar de los locales de la planta o fábrica.

Para permitir la activación, el producto o componente 140 se ha dotado de un elemento 141 no clonable. En la realización de la Figura 1, el elemento 141 no clonable forma parte del microchip 140, pero puede ser proporcionado igualmente en cualquier parte del producto o componente. Por ejemplo, el elemento 141 no clonable puede ser proporcionado en la placa madre de un ordenador u ordenador personal portátil, y estar previsto para la activación de un chip particular también presente en el ordenador.

El elemento 141 no clonable tiene la misión de producir una o más salidas ruidosas, indicadas como R_1, ..., R_n en la Figura 1. La(s) salida(s) es (son) suministrada(s) al sistema 110, en esta realización transmitiéndola(s) por una red 120 de comunicaciones tal como Internet. Por supuesto, se puede utilizar igualmente una línea de teléfono o cualquier otro medio de comunicación.

El sistema 110 computa datos auxiliares HD basados en las salidas ruidosas que recibe, y proporciona estos datos auxiliares HD de nuevo a la posición remota 130. En la posición remota 130, los datos auxiliares HD se ponen a disposición del producto o componente 140, por ejemplo almacenándolos en una memoria 143 del microchip.

Los datos auxiliares transforman la una o más salidas ruidosas en un valor simple que debe corresponder con el elemento de datos de activación correcta. Si se obtiene, en efecto, el elemento de datos de activación correcta, la funcionalidad puede ser habilitada. Existen muchas formas en las que esto puede ser realizado.

Según se ha mencionado en lo que antecede, la activación se implementa en una realización comparando el valor simple con un código predefinido disponible en el bloque de IP. Si no se emparejan los dos, no se habilita la función.

Si el producto o componente 140 es un programa de software o una corriente de datos para una FAPA, el valor simple puede ser utilizado también como clave para desbloquear o descodificar todo o una parte del producto o componente 140.

El valor simple puede indicar también una pluralidad de funciones que han de ser habilitadas o deshabilitadas. Esto se puede realizar tratando el valor simple como una secuencia de indicadores, de los que cada uno indica si una función particular debe ser habilitada o no. Una manera fácil de llevar esto a cabo consiste en utilizar una máscara de bits. Por ejemplo, la máscara de bits 00101101 de ocho bits, indica que las dos primeras, la cuarta y la séptima funciones están deshabilitadas, y que la tercera, la quinta, la sexta y la octava funciones están habilitadas.

Este valor simple puede ser utilizado también como una clave necesaria para procesar una entrada proporcionada al producto o componente 140, por ejemplo como clave de descodificación para un contenido audiovisual que ha de ser descodificado o para autenticar el producto o componente 140 en un servidor remoto (no representado) con el que se deben intercambiar datos.

Exactamente qué función (o qué funciones) se activa(n) y cómo, es accesorio para la invención. Los principios de la invención según se reivindica, pueden ser aplicados para habilitar o activar cualquier funcionalidad en cualquier clase de dispositivo. Sin embargo, a los efectos de ilustración de la invención, se proporcionan los siguientes ejemplos:

- Habilitar el uso de un chip de codificación o descodificación de audio y/o video de alto rendimiento, o un programa de software.
- Habilitar la comunicación por una red inalámbrica tal como 802.11g.
- Deshabilitar una limitación artificial en la funcionalidad del producto, tal como una limitación de tiempo o una limitación sobre la cantidad de datos que pueden ser transmitidos por unidad de tiempo.
- Permitir la descarga de mejoras o actualizaciones para el producto o su funcionalidad.
- Habilitar comunicaciones por enlaces tales como HDTV que utiliza el protocolo de protección de copia HDMI; la activación en este caso ocurre adquiriendo la clave de autenticación de derecho.
- Habilitar la funcionalidad de un ASIC, FPGA o circuito similar, por ejemplo habilitando el uso de claves de dispositivo encriptadas con el dispositivo para descodificación del contenido audiovisual.
- Habilitar un modelo de pago por-uso en el que el cliente solamente paga por la funcionalidad que elija. Cada función puede ser habilitada individualmente, y el código de autorización para cada función se adquiere por separado.

El elemento 141 no clonable es conocido en sí mismo. Una denominación para tales componentes es el de Funciones Físicas Aleatorias (No Clonables) o PUFs. Una PUF es un elemento físico complejo que comprende muchos componentes distribuidos aleatoriamente. Cuando se analiza con supuestos adecuados, la física compleja que gobierna la interacción entre el elemento físico y el supuesto, por ejemplo múltiples ondas de dispersión en un medio desordenado, conduce a una salida, o respuesta, diferente de búsqueda aleatoria, para cada supuesto separado.

Las respuestas recibidas a partir de la señal, son susceptibles de ruido y perturbaciones, que causan diferencias en las respuestas cada vez que se presenta un supuesto simple a la PUF. Un elemento de datos auxiliares proporciona redundancia para transformar esta respuesta múltiple, ruidosa, en un valor simple. La estructura compleja de pequeña escala de la señal física hace que sea difícil producir una copia física.

Adicionalmente a la literatura ya mencionada, ejemplos de PUFs se divulgan en:

1. R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, “Funciones Físicas de Un Solo Sentido”, Science vol. 297, pp- 2026, (2002)
2. P. Tuyls, B. Skoric, S. Stallinga, A. H. Akkermans, W. Ophey, “Información - Análisis de Seguridad Teórica de Funciones Físicas No Clonables”, Financial Cryptography FC’05, LNCS 3570, Springer-Verlag pp. 141 (2005)
3. B. Skoric, P. Tuyls W. Ophey, “Extracción de clave robusta a partir de Funciones Físicas No Clonables”, Applied Cryptography and Network Security ACNS 2005, LNCS 3531, pp. 407-422 (2005)
4. P. Tuyls, B. Skoric, G.J. Schrijen, R. Wolters, J. van Geloven, N. Verhaegh, H. Kretschmann, “Hardware a prueba de lectura desde recubrimientos protectores”, CHES 2006 para aparecer (2006)
5. B. Gassend, D. Clarke, M. van Dijk, S. Devadas, “Funciones Aleatorias Físicas de Silicio”, 9ª Conf. ACM sobre Ordenador y Seguridad de Comunicación (2002)
6. P. Tuyls, B. Skoric, “Generación de Calve Secreta a partir de Física Clásica”, Book Chapter, Hardware Technology Drivers for Ambient Intelligence, Kluwer (2005)

En la actualidad se conocen varios sistemas físicos en los que se pueden basar las PUFs. Los tipos principales son PUFs ópticas (véase la referencia 1), PUFs de recubrimiento (referencia 4), PUFs de silicio (referencia 5) y PUFs acústicas (referencia 6). De hecho, cualquier sistema físico con las propiedades que siguen, puede ser utilizado como PUF si tiene las siguientes propiedades:

- Barato y fácil de fabricar, y que incluya variaciones incontrolables aleatorias del proceso de fabricación.

- Poco práctico para caracterizar y modelizar
- Gran espacio de entrada/ salida

Aunque la presente invención es aplicable a todos los tipos de PUF, considérese como ejemplo el ejemplo específico de la PUF óptica como ejemplo concreto de los conceptos aquí descritos. Las PUFs ópticas consisten en un material de transporte que consiste en partículas de dispersión distribuidas aleatoriamente. La aleatoriedad está proporcionada en este caso por la unicidad y la imprevisibilidad de patrones de moteado que resultan de la dispersión múltiple de luz láser en un medio óptico distorsionado (referencia 2). Para una longitud de onda fija de la luz incidente, la entrada es el ángulo de incidencia, la distancia focal, el patrón de máscara o cualquier otro cambio reproducible en el frente de la onda. La salida es el patrón de moteado resultante. Incluso dados todos los detalles precisos de las dispersiones, resulta extremadamente difícil recuperar un patrón de moteado particular. Para más información sobre las PUFs y la reconstrucción de datos auxiliares para estabilizar respuestas de PUF, el lector debe dirigirse a la literatura mencionada anteriormente.

Para evitar que un atacante en la posición remota 130, por ejemplo el fabricante que opera una fábrica, acceda a la una o más salidas ruidosas y/o a los datos auxiliares, cualquiera de ellas o todas podrían ser codificadas utilizando una clave o algoritmo desconocido por este atacante. Por ejemplo, el producto o componente 140 puede aplicar una codificación simple basada en XOR a la una o más salidas ruidosas utilizando una clave fija. En disposiciones más complejas, el producto o componente 140 y el sistema 110 pueden establecer un canal autenticado seguro para intercambiar de forma segura la una o más salidas ruidosas y/o los datos auxiliares.

Una realización preferida consiste en hacer que el sistema 110 produzca un elemento de autenticación para los datos auxiliares, por ejemplo creando una signatura digital o código de autenticación de mensaje para los datos auxiliares utilizando una clave secreta conocida por el sistema 110. Dependiendo del algoritmo o la tecnología de autenticación que se utilice, el elemento de autenticación puede ser transmitido junto con, o en lugar de, los datos auxiliares sin formato. Por ejemplo, cuando se genera una signatura digital utilizando un algoritmo como RSA, se puede utilizar la signatura digital en vez de los propios datos auxiliares puesto que los datos auxiliares son recuperados cuando la signatura digital se verifica con éxito.

El producto o componente 140, en la presente realización, está configurado de modo que emplea solamente los datos auxiliares si se puede verificar la autenticidad de los datos auxiliares utilizando este elemento de autenticación. Cuando se utilizan signaturas digitales criptográficas de clave pública/ secreta, el producto o componente 140 almacena una clave pública correspondiente a la clave secreta mencionada anteriormente, para permitir tal verificación. La verificación de criptografía de clave pública/ secreta y de signatura digital, es bien conocida y por lo tanto no va a ser elaborada de manera más detallada.

Esto impide el suministro de datos auxiliares por partes no autorizadas. Incluso aunque una tercera parte cualquiera gestione determinar cómo producir datos auxiliares para habilitar la funcionalidad particular, no puede crear el elemento de autenticación correcta, y por lo tanto estará incapacitada para activar la funcionalidad.

La Figura 2 muestra una realización adicional del sistema 110 en la que se introduce una tercera parte 200. La tercera parte 200 proporciona un elemento de autenticación al sistema 110, cuyo elemento de autenticación se utiliza para establecer la autenticidad de los datos auxiliares. El sistema 110, a su vez, transmite el elemento de autenticación a la localización remota.

Una realización preferida consiste en hacer que la tercera parte 200 produzca una signatura digital o codificación para los datos auxiliares codificando los datos auxiliares con una clave secreta conocida por la tercera parte. Esto ha sido mostrado en la Figura mediante $E_{SKTP}(HD)$, abreviatura de cifrado por la Tercera Parte de los Datos Auxiliares con la Clave Secreta.

Dependiendo del algoritmo de la signatura digital o de la tecnología utilizada, el elemento de autenticación puede ser transmitido junto con, o en lugar de, los datos auxiliares sin formato.

El producto o componente 140 de esta realización está configurado para que emplee solamente los datos auxiliares si se puede verificar la autenticidad de los datos auxiliares utilizando este elemento de autenticación. En la realización preferida mencionada anteriormente, el producto o componente 140 almacena una clave pública correspondiente a la clave secreta mencionada anteriormente para habilitar tal verificación.

La Figura 3 muestra una realización adicional del sistema 110 en la que los datos auxiliares son codificados con anterioridad a transmitirlos a la tercera parte. Los datos auxiliares pueden ser codificados utilizando criptografía simétrica o asimétrica. Esto impide que la tercera parte observe los datos auxiliares reales. Esto ha sido mostrado mediante $E_{PKC}(HD)$, abreviatura de codificación con una Clave Pública del Componente. La tercera parte 200 produce una signatura digital para estos datos auxiliares codificados: $E_{SKTP}(E_{PKC}(HD))$.

El producto o componente 140 almacena ahora una clave secreta correspondiente a la clave pública PKC mencionada anteriormente, por ejemplo en la memoria 143. El producto o componente 140 de esta realización está configurado para que emplee solamente los datos auxiliares si (1) el elemento de autenticación $E_{PKC}(HD)$ puede ser

descodificado con éxito utilizando la clave secreta antes mencionadas, y (2) la autenticidad de los datos auxiliares HD puede ser verificada utilizando este elemento de autenticación.

La Figura 4 muestra una realización adicional del sistema 110 en la que la posición remota 130 incluye un elemento de autenticación remota. El sistema 110 solamente proporciona ahora los datos auxiliares si los datos auxiliares pueden ser autenticados con éxito utilizando el elemento de autenticación remota. Con preferencia se produce una signatura digital para las respuestas utilizando una clave secreta conocida, ya sea en la posición remota 130 o ya sea en el producto o componente 140. Esto ha sido mostrado en la Figura 4 mediante $E_{SKRL}(R_1, ..., R_n)$, abreviatura de codificación con la Clave Secreta de la Posición Remota de las Respuestas.

En otra realización (no representada), la una o más salidas ruidosas $R_1, ..., R_n$ recibidas se comparan con la pluralidad de salidas ruidosas previamente recibidas, y solamente se proporcionan los datos auxiliares si la una o más salidas ruidosas no han sido recibidas con anterioridad. El sistema 110 de esta realización puede estar equipado con una base de datos para almacenar las salidas ruidosas recibidas. Una representación abreviada (por ejemplo, una versión con hash) de las salidas ruidosas, puede ser almacenada en lugar de las propias salidas ruidosas para reducir los requisitos de almacenamiento. Por ejemplo, se puede aplicar una función hash a las salidas ruidosas, y la salida de esta función puede ser almacenada. El emparejamiento de los hashes es mucho más eficiente e incluso permite determinar si exactamente las mismas respuestas ruidosas han sido recibidas con anterioridad.

Se debe apreciar que las realizaciones mencionadas en lo que antecede ilustran, en vez de limitar, la invención, y que los expertos en la materia estarán capacitados para diseñar muchas realizaciones alternativas sin apartarse del alcance de las reivindicaciones anexas. Por ejemplo, las realizaciones de las Figuras 2, 3 y/o 4 pueden combinarse para combinar ventajosamente los beneficios de cualesquiera, o de todas ellas, entre sí. Según otro ejemplo, los datos auxiliares pueden ser transmitidos a una segunda posición remota diferente de la posición remota desde la que han sido recibidas la una o más respuestas.

En las reivindicaciones, cualquiera de los signos de referencia puestos entre paréntesis no debe ser entendido como limitativo de la reivindicación. El término “que comprende” no excluye la presencia de elementos o de etapas distintas de las relacionadas en una reivindicación. La palabra “un” o “una” precediendo a un elemento no excluye la presencia de una pluralidad de tales elementos. La invención puede ser implementada por medio de hardware que comprenda varios elementos distintos, y por medio de un ordenador programado adecuadamente.

En una reivindicación de dispositivo que enumere diversos medios, varios de esos medios pueden estar materializados por uno, y mismo, elemento de hardware. El mero hecho de que se mencionen determinadas medidas en diferentes reivindicaciones mutuamente dependientes, no indica que no se pueda utilizar una combinación de esas medidas ventajosamente.

REIVINDICACIONES

1.- Un procedimiento de activación controlada de al menos una función en un producto o componente en una posición remota, cuya activación requiere que un elemento de datos de activación correcta se encuentre disponible en el producto o componente, **caracterizado por** recibir una o más salidas ruidosas de un elemento no clonable asociado al componente desde la posición remota, siendo las salidas del elemento no clonable susceptibles de ruido y perturbaciones, y proporcionar datos auxiliares a la posición remota para transformar la una o más salidas ruidosas en un valor simple que corresponda con el elemento de datos de activación correcta.

2.- El procedimiento de la reivindicación 1, que comprende además transmitir un elemento de autenticación, para establecer la autenticidad de los datos auxiliares, hasta la posición remota.

3.- El procedimiento de la reivindicación 2, en el que el elemento de autenticación se obtiene transmitiendo los datos auxiliares a una tercera parte, y recibiendo el elemento de autenticación como respuesta desde la tercera parte.

4.- El procedimiento de la reivindicación 3, en el que los datos auxiliares son codificados con anterioridad a transmitirlos a la tercera parte.

5.- El procedimiento de la reivindicación 1, que comprende además recibir un elemento de autenticación remota desde la posición remota, y proporcionar solamente los datos auxiliares si los datos auxiliares pueden ser autenticados con éxito utilizando el elemento de autenticación remota.

6.- El procedimiento de la reivindicación 1, en el que los datos auxiliares son transmitidos a una segunda posición remota diferente de la posición remota desde la que han sido recibidas la una o más respuestas.

7.- El procedimiento de la reivindicación 1, en el que la una o más salidas ruidosas recibidas son comparadas con la pluralidad de salidas ruidosas previamente recibidas, y los datos auxiliares se suministran solamente si la una o más salidas ruidosas no han sido recibidas con anterioridad.

8.- El procedimiento de la reivindicación 1, en el que el valor simple se utiliza como clave de descodificación o como clave de autenticación.

9.- El procedimiento de la reivindicación 1, en el que el valor simple se utiliza como clave para desbloquear o descodificar todo o parte del producto o componente.

10.- El procedimiento de la reivindicación 9, en el que el producto o componente es un programa de software o una corriente de datos para una FPGA.

11.- Un sistema para la activación controlada de al menos una función en un producto o componente en una posición remota, cuya activación requiere que un elemento de datos de activación correcta esté disponible en el producto o componente, **caracterizado por** medios de recepción para recibir una o más salidas ruidosas de un elemento no clonable asociado al componente desde la posición remota, siendo las salidas del elemento no clonable susceptibles de ruido y perturbaciones, y medios para proporcionar datos auxiliares a la posición remota para transformar la una o más salidas ruidosas en un valor simple que corresponda con el elemento de datos de activación correcta.

12.- El sistema de la reivindicación 11, en el que los medios de recepción están configurados para recibir la una o más salidas ruidosas transmitidas por una red de comunicaciones.

13.- El sistema de la reivindicación 12, en el que la red de comunicaciones es Internet.

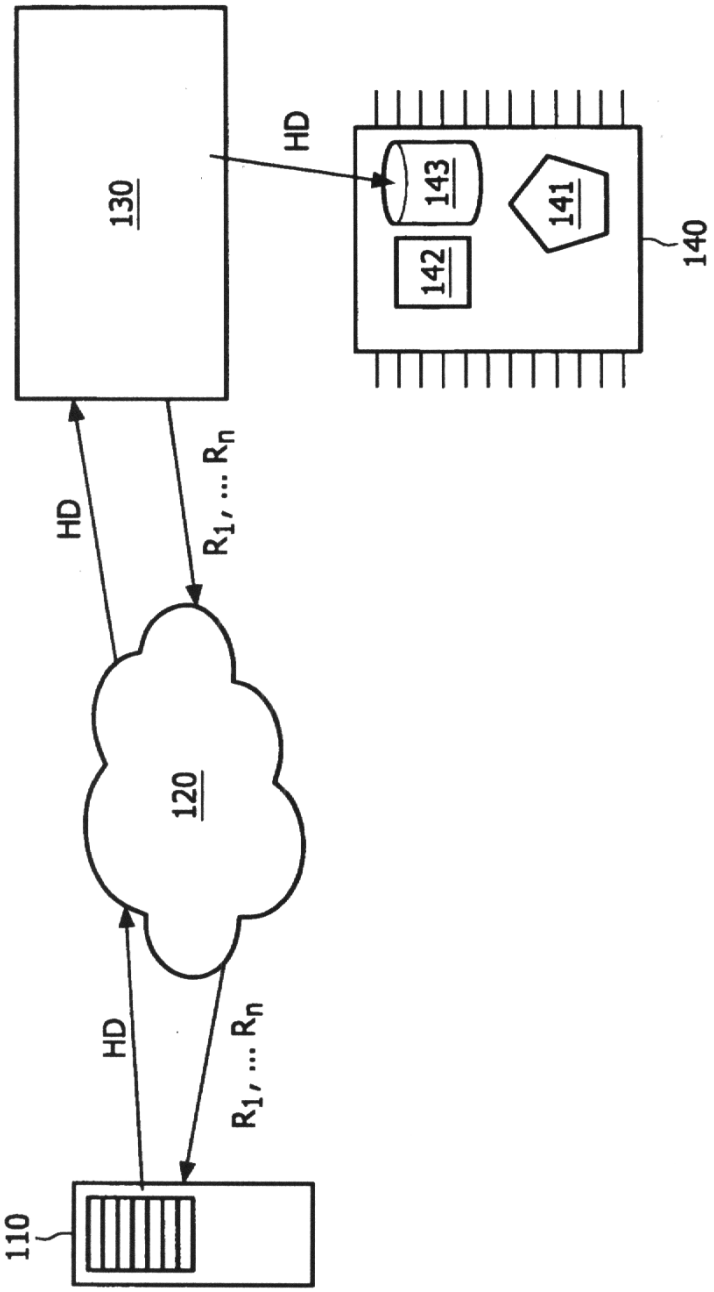

FIG. 1

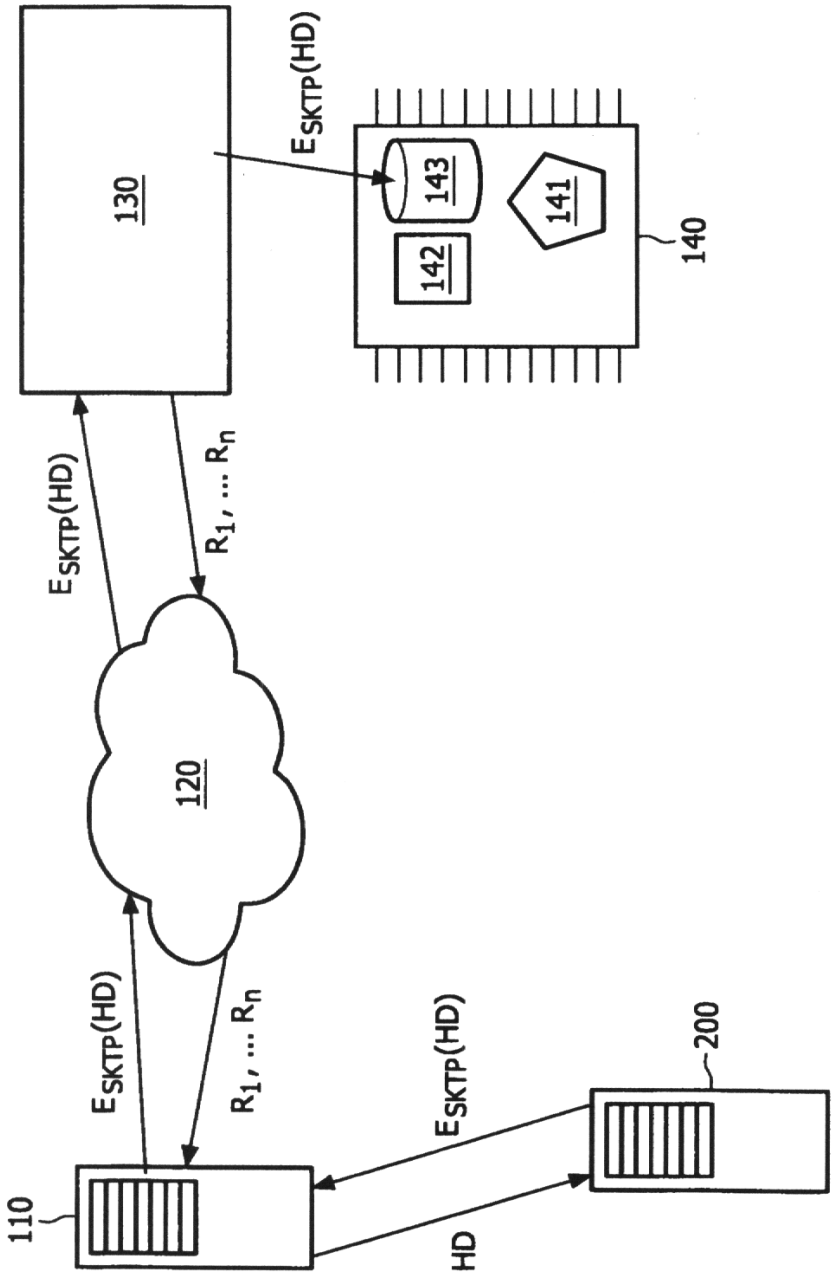
130
$E_{SKTP}(HD)$
143
141
142
140
$E_{SKTP}(HD)$
$R_1, \ldots R_n$
120
$E_{SKTP}(HD)$
$R_1, \ldots R_n$
$E_{SKTP}(HD)$
200
110
HD

FIG. 2

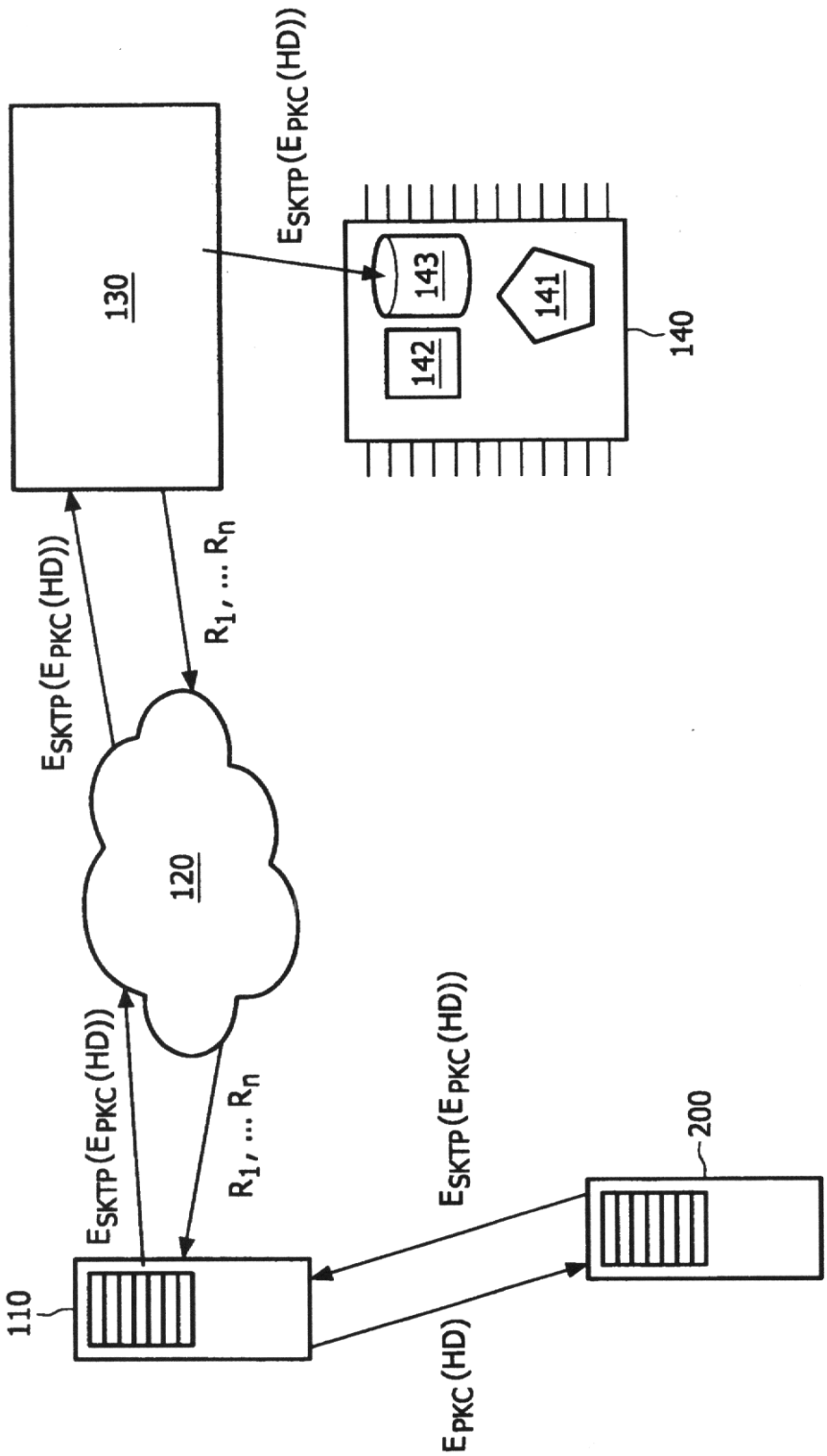
130
$E_{SKTP}(E_{PKC}(HD))$
143
141
142
140
$E_{SKTP}(E_{PKC}(HD))$
$R_1, \ldots R_n$
120
$E_{SKTP}(E_{PKC}(HD))$
$R_1, \ldots R_n$
$E_{SKTP}(E_{PKC}(HD))$
200
110
$E_{PKC}(HD)$

FIG. 3

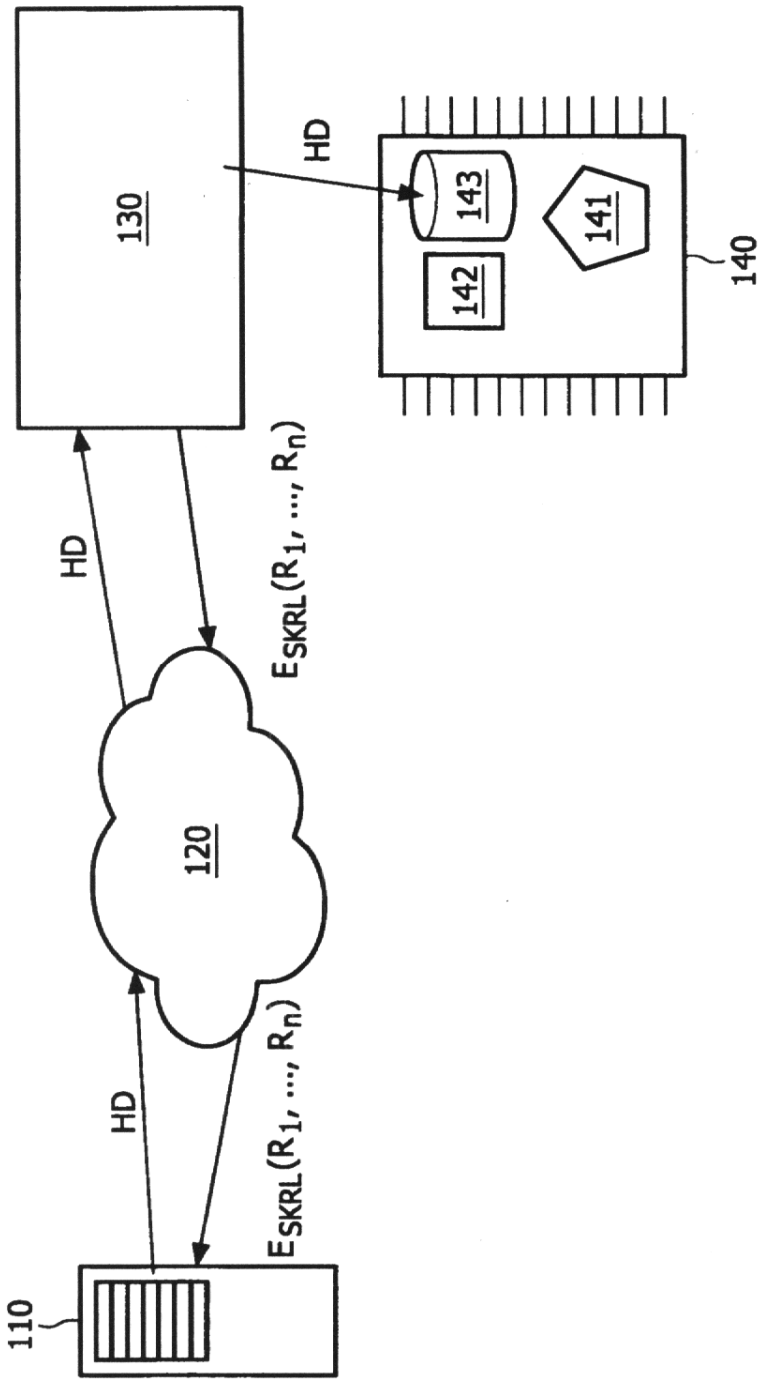

FIG. 4