(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 730 691**

(51) Int. CI.:

H04L 9/30 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.02.2013 PCT/EP2013/000421**

(87) Fecha y número de publicación internacional: **19.09.2013 WO13135337**

(96) Fecha de presentación y número de la solicitud europea: **13.02.2013 E 13706171 (9)**

(97) Fecha y número de publicación de la concesión europea: **10.04.2019 EP 2826199**

(54) Título: **Procedimiento y sistema para la comunicación segura entre una etiqueta RFID y un dispositivo de lectura**

(30) Prioridad:

16.03.2012 DE 102012005427

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.11.2019

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstraße 159
81677 München, DE

(72) Inventor/es:

HINZ, WALTER;
FINKENZELLER, KLAUS y
SEYSEN, MARTIN

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Procedimiento y sistema para la comunicación segura entre una etiqueta RFID y un dispositivo de lectura

La invención se refiere a un procedimiento y un sistema para la comunicación segura entre una etiqueta RFID y un dispositivo de lectura a través de la interfaz de aire así como a correspondientes etiquetas RFID y correspondientes dispositivos de lectura.

La tecnología RFID ("radio frequency identification") hace posible, en particular, la identificación automática de personas y objetos y encuentra un uso creciente en multitud de aplicaciones como, por ejemplo, en la gestión de la cadena de suministro, en sistemas de control de acceso, en sistemas de seguridad antirrobo de mercancías, en emisión electrónica de recibos y similares. Un sistema RFID normalmente consiste en un soporte de datos portátil en la forma de una etiqueta RFID (también denominado transpondedor) que lleva una persona consigo o se fija a un objeto y en el que se almacena un código de identificación (para el experto también conocido como UID ("Unique-ID), TID ("Tag-ID"), o UII ("Unique Item Identifier")) que identifica inequívocamente la etiqueta RFID y/o el objeto, así como en un dispositivo de lectura para leer sin contacto el código de identificación de la etiqueta RFID. En este caso, el dispositivo de lectura normalmente es sólo un dispositivo de lectura de múltiples dispositivos de lectura que están instalados en distintos sitios y pueden acceder a datos almacenados ahí de multitud de etiquetas RFID por medio de un sistema de fondo.

En particular, las etiquetas RFID asequibles y previstas para aplicaciones de logística y para la gestión de la cadena de suministro, las cuales normalmente se tratan de etiquetas RFID pasivas, en las que la energía requerida para la operación se extrae del campo electromagnético de un dispositivo de lectura, no ofrecen frecuentemente ninguna función criptográfica, de manera que una autentificación de una etiqueta RFID respecto a un dispositivo de lectura en tales etiquetas RFID no es posible. Este es el caso, por ejemplo, en las etiquetas RFID UHF que son conocidas para el experto con el nombre de etiquetas EPC Clase 1 Gen 2, es decir etiquetas RFID que están configuradas según la norma EPC Clase 1 Generación 2 o la nueva norma ISO/IEC 18000-63. Como es conocido para el experto, el término "etiquetas EPC Clase 1 Gen 2" comprende también etiquetas según la norma ISO/IEC 18000-63. En tales etiquetas RFID el código de identificación inequívoco se denomina como EPC ("Electronic Product Code"), tratándose normalmente de una secuencia de bits consistente en 96 bits almacenada en una etiqueta RFID respectiva. El EPC se transmite a un dispositivo de lectura en un proceso de lectura de una etiqueta RFID en texto simple sin autentificación y puede captarse por tanto activamente, mediante un dispositivo de lectura de un tercero no autorizado, como también pasivamente, al interceptar un tercero el canal de comunicación no protegido, es decir, la interfaz de aire, entre la etiqueta RFID y un dispositivo de lectura.

Esto lleva a dos problemas potenciales, que son, por una parte, que la presencia y la posición de una etiqueta RFID puede ser detectada y seguida por un tercero no autorizado, lo que también se denomina como seguimiento ("tracking") de una etiqueta RFID y, por otra parte, que un tercero puede copiar el EPC leído en una nueva etiqueta RFID falsificada y entonces exhibir la nueva etiqueta RFID falsificada como la etiqueta en la que se leyó originalmente el EPC, lo que se denomina también como clonado de una etiqueta RFID.

Para asegurar la comunicación entre una etiqueta RFID y un dispositivo de lectura se ofrecen procedimientos criptográficos que, por una parte, hacen posible una autentificación unidireccional o bidireccional entre la etiqueta RFID y el dispositivo de lectura y, por otra parte, un encriptado de la comunicación a través de la interfaz de aire. Los procedimientos criptográficos se subdividen en procedimientos simétricos, en los que el emisor y el receptor utilizan la misma clave privada, y procedimientos asimétricos o de clave pública, en los que el emisor utiliza una clave pública ("public key") y el receptor una clave privada ("private key"). Sin embargo, en los procedimientos simétricos se sabe que existe el problema de que la clave secreta conjunta debe almacenarse de forma segura tanto en una etiqueta RFID como también en un dispositivo de lectura o un sistema de fondo conectado al mismo, lo que en los sistemas con múltiples etiquetas RFID y múltiples dispositivos de lectura hace precisa una gestión de claves compleja, de la que se prescinde en procedimientos asimétricos o de clave pública. De una gestión de claves de este tipo también puede prescindirse en los sistemas que utilizan un procedimiento simétrico, en el caso de que en todas las etiquetas RFID y en el sistema de fondo se almacene la misma clave general. Sin embargo, esto encierra el riesgo de que el sistema queda desprotegido tan pronto como la clave general de una etiqueta RFID se haya detectado. Este riesgo no existe con los procedimientos de clave pública.

Un procedimiento conocido de clave pública es el procedimiento de Rabin que, como el procedimiento RSA frecuentemente utilizado, usa como base la exponenciación modular. Dado que en el procedimiento de Rabin el cálculo del encriptado es esencialmente más simple, es decir, menos intensivo computacionalmente que el procedimiento RSA, el procedimiento de Rabin se prefiere respecto al procedimiento RSA especialmente donde la entidad que realiza el encriptado, es decir, el emisor de un mensaje encriptado, sólo dispone de una capacidad de procesamiento limitada, como es el caso de, por ejemplo, una etiqueta RFID de recursos limitados que debe comunicarse de forma segura con un dispositivo de lectura conectado a un sistema de fondo.

En el procedimiento de Rabin, la clave secreta consiste en dos números primos p y q en la práctica seleccionados suficientemente grandes que están vinculados entre sí por medio de una determinada condición de congruencia. El

producto $n = p \cdot q$ de los dos números primos p y q define los módulos o el módulo n y al mismo tiempo representa la clave pública. Convenientemente, los números primos p y q son aproximadamente del mismo tamaño. Según el procedimiento de Rabin, un texto simple M a ser transmitido es encriptado mediante elevación al cuadrado modular y aplicación de la operación de módulo, es decir, el texto cifrado C se deriva a partir del texto simple M según la siguiente fórmula: $C = M^2 \bmod n$.

La seguridad del procedimiento de Rabin se basa en que el cálculo de la raíz cuadrada modular a partir del texto cifrado C es muy difícil sin conocer los números primos p y q. Sin embargo, este es sólo el caso de que el texto simple M no sea sustancialmente más pequeño que el módulo n. Mediante la operación de módulo con la elevación al cuadrado se evita que sea posible un desencriptado por simple extracción de la raíz.

Dado que en el procedimiento de Rabin el encriptado por el emisor implica una elevación al cuadrado modular, para el desencriptado el receptor tiene que calcular la raíz cuadrada modular del texto cifrado C. En este sentido, puede utilizarse de manera conocida el teorema del resto chino ("chinese remainder theorem", CRT). Como es conocido para el experto, resultan con ello cuatro raíces cuadradas, de las cuales una debe seleccionarse como el texto simple M original. Para ello, el texto simple M "correcto" puede identificarse al receptor por medio de, por ejemplo, un identificador adecuado, una suma de comprobación o similares.

Como resulta de la fórmula descrita previamente para el cálculo del texto cifrado C en el procedimiento de Rabin, para la realización de la operación de módulo el emisor normalmente debe realizar una división de números grandes. Sin embargo, una división de números grandes de este tipo sólo puede realizarse en microprocesadores simples, como los utilizados con etiquetas RFID, con gran dificultad.

En la publicación "A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes" de Y. Oren y M. Feldhofer en D.A. Basin, S. Capkun, y W.Lee, editores, WISEC, páginas 59-68, ACM 2009, con el nombre de procedimientos WIPR se propone una modificación del procedimiento de Rabin convencional que, en particular, está previsto para asegurar la comunicación entre una etiqueta RFID de recursos limitados con un procesador simple y un dispositivo de lectura. En comparación con este, el procedimiento de Rabin convencional descrito previamente, el procedimiento WIPR presenta la ventaja de que para calcular el texto cifrado en vez de una división de grandes números costosa que es muy intensiva computacionalmente y que, por tanto, apenas puede ser implementada en microprocesadores simples, como los que se encuentran en etiquetas RFID normalmente, se utilizan multiplicaciones de grandes números, las cuales son sustancialmente más rápidas de ejecutar como divisiones y también pueden ser implementadas en hardware de forma más simple.

De acuerdo con el procedimiento WIPR, el texto cifrado C' se calcula al generar el emisor, por ejemplo, una etiqueta RFID, un número aleatorio r, multiplica éste por el módulo n y el resultado se suma al cuadrado del texto simple M, es decir, $C' = M^2 + r \cdot n$. Con ello, un código de identificación de la etiqueta RFID se incorpora en el texto simple M y el tamaño del número aleatorio r se selecciona de tal modo que el producto $r \cdot n$ sea más del doble que el módulo n. Por tanto, en comparación con el procedimiento de Rabin convencional, en el procedimiento WIPR, el cuadrado del texto simple M no queda enmascarado por la realización de la operación de módulo que implica una división de grandes números, sino por la adición del producto $r \cdot n$ con el número aleatorio r seleccionado adecuadamente.

En la publicación A. Shamir, "Memory Efficient Variants of Public-Key Schemes for Smart Card Applications", en A. D. Santis, editor, Advances in Cryptology - EUROCRYPT '94, Springer LNCS, Vol. 950, páginas 445-449, se ha mostrado que un procedimiento como el procedimiento WIPR es tan seguro como el procedimiento de Rabin convencional si el número aleatorio r se elige aleatoriamente de un intervalo suficientemente grande.

Sin embargo, en el procedimiento WIPR la ventaja de evitar una división de grandes números se compensa con el hecho de que el texto cifrado C', debido a la omisión de la operación de módulo en la elevación al cuadrado del texto simple M y debido al producto del módulo n por el número aleatorio r seleccionado suficientemente grande, será normalmente muy grande, lo que ralentiza el proceso de autentificación entre una etiqueta RFID y un dispositivo de lectura, puesto que una cantidad de datos mayor debe transmitirse desde la etiqueta RFID al dispositivo de lectura.

La publicación de Patente DE 198 20 605 divulga un procedimiento de Rabin para la verificación de una firma, configurado ventajosamente para dispositivos de baja capacidad de cálculo mediante multiplicación de Montgomery.

A la vista de estos antecedentes la presente invención plantea el problema de proporcionar un procedimiento mejorado y un sistema mejorado para la comunicación segura entre una etiqueta RFID y un dispositivo de lectura a través de la interfaz de aire que protege la etiqueta RFID, en particular, respecto a su seguimiento y/o clonación. Además, se debe proporcionar una etiqueta RFID diseñada correspondientemente así como un dispositivo de lectura diseñado correspondientemente.

Este cometido se consigue de acuerdo con la invención mediante el objeto de las reivindicaciones independientes. En las reivindicaciones dependientes se definen desarrollos ventajosos de la invención.

La invención se basa en la idea de que para la comunicación segura entre una etiqueta RFID y un dispositivo de lectura se utiliza una modificación del procedimiento de Rabin en el que en el marco del encriptado de un texto simple *M*, en el que se incorpora un elemento de identificación de la etiqueta RFID o un objeto provisto del mismo, de la etiqueta RFID en vez del cuadrado del texto simple *M* módulo *n*, es decir, M^2 mod*n*, se calcula el residuo de Montgomery ("Montgomery reduction") del cuadrado del texto simple *M* módulo *n*, respecto a una base de Montgomery *R*, es decir, $C^* = M^2 R^{-1}$ mod*n*, y el texto cifrado *C** resultante de ello se utiliza para la autentificación de la etiqueta RFID. Se trata en el módulo $n = p \cdot q$ de la clave pública del dispositivo de lectura, en los números primos p, q, de la clave privada del dispositivo de lectura y en la base de Montgomery *R* es un número entero que es mayor que el módulo *n*. Aquí la base de Montgomery es normalmente una potencia de dos.

En base a la idea de la presente invención descrita previamente, de acuerdo con un primer aspecto de la invención se proporciona un procedimiento para la comunicación segura entre una etiqueta RFID y un dispositivo de lectura, tal que el procedimiento comprende las siguientes etapas que se realizan en la etiqueta RFID. El encriptado de un texto simple *M*, en el que se incorpora un elemento de identificación de la etiqueta RFID o un objeto provisto del mismo, para el cálculo de un texto cifrado *C**, usando el residuo de Montgomery del cuadrado del texto simple *M* de módulo *n* respecto a una base de Montgomery *R*, es decir, $C^* = M^2 R^{-1}$ mod*n*, y el envío de un mensaje de autentificación al dispositivo de lectura, estando basado el mensaje de autentificación en el texto cifrado *C**.

Adicionalmente, en base al concepto de la idea descrita previamente, de acuerdo con un segundo aspecto de la invención se proporciona un procedimiento para la comunicación segura entre una etiqueta RFID y un dispositivo de lectura, tal que el procedimiento comprende las siguientes etapas que son realizadas en el dispositivo de lectura. La recepción de un mensaje de autentificación de la etiqueta RFID que está basado en un texto simple *M* encriptado, en el que se ha incluido un elemento de identificación de la etiqueta RFID o un objeto provisto del mismo, y el desencriptado del texto simple *M* encriptado, comprendiendo la etapa del desencriptado la multiplicación del texto simple *M* encriptado por una base de Montgomery *R* y la realización subsiguiente de la operación de módulo con el módulo *n*. Preferiblemente, la etapa del desencriptado comprende adicionalmente el cálculo subsiguiente de la raíz cuadrada de módulo n análogamente al procedimiento de Rabin convencional.

Además, en base al concepto descrito previamente de la presente invención, de acuerdo con un tercer aspecto de la invención se proporciona una etiqueta RFID para la comunicación segura con un dispositivo de lectura. Con ello la etiqueta RFID comprende una unidad de procesador y una unidad de almacenamiento. En la unidad de almacenamiento se almacena un elemento de identificación. La unidad de procesador está configurada para que un texto simple *M*, en el que se incorpora el elemento de identificación de la etiqueta RFID o un objeto provisto del mismo, para el cálculo de un texto cifrado *C** a ser encriptado, siendo calculado el residuo de Montgomery del cuadrado del texto simple *M* de módulo *n* respecto a una base de Montgomery *R*, es decir, $C^* = M^2 R^{-1}$ modn y un mensaje de autentificación a ser enviado al dispositivo de lectura, estando basado el mensaje de autentificación en el texto cifrado *C**.

Adicionalmente, en base a la idea descrita previamente de la presente invención, de acuerdo con un cuarto aspecto de la invención se proporciona un dispositivo de lectura para la comunicación segura con una etiqueta RFID. El dispositivo de lectura comprende una unidad de procesador que está configurada para recibir un mensaje de autentificación de la etiqueta RFID que está basado en un texto simple *M* encriptado, en el que se ha incorporado un elemento de identificación de la etiqueta RFID o un objeto provisto del mismo, y desencriptar el texto simple encriptado, tal que en el desencriptado el texto simple *M* encriptado se multiplica por una base de Montgomery *R* y a continuación se realiza la operación de módulo con el módulo *n*. Preferiblemente, la unidad de procesador del dispositivo de lectura para el desencriptado del texto simple encriptado está configurado adicionalmente para a continuación obtener la raíz cuadrada de módulo *n* análogamente al procedimiento de Rabin convencional.

Finalmente, en base a la idea descrita previamente de la presente invención, de acuerdo con un quinto aspecto de la invención se proporciona un sistema para la comunicación segura con al menos una etiqueta RFID según el tercer aspecto de la invención y al menos un dispositivo de lectura según el cuarto aspecto de la invención.

Como se ha mencionado previamente, el módulo $n = p \cdot q$ es la clave pública del dispositivo de lectura, los números primos *p*, *q* la clave privada del dispositivo de lectura y la base de Montgomery *R* un número entero que es mayor que el módulo *n*.

Preferiblemente, el mensaje de autentificación transmitido al dispositivo de lectura desde la etiqueta RFID contiene el texto simple M encriptado en la forma del texto cifrado *C** con $C^* = M^2 R^{-1}$ mod*n*.

Según formas de realización preferibles de la invención, la invención incorpora adicionalmente en el texto simple M un primer número aleatorio *RND1* generado por el dispositivo de lectura y un segundo número aleatorio *RND2* generado por la etiqueta RFID. Con ello, el primer número aleatorio *RND1*, preferiblemente, se transmite a la etiqueta RFID como demanda ("challenge") en el marco de un procedimiento de demanda-respuesta ("challenge-response"). En esta configuración preferible, los datos incorporados en el texto simple *M*, en particular, el elemento de identificación de la etiqueta RFID, el primer número aleatorio *RND1* y el segundo número aleatorio *RND2* son, preferiblemente, mezclados por medio de una operación de intercalado ("interleaving"), con objeto de distribuir los

datos aleatorios procedentes del dispositivo de lectura y de la etiqueta RFID aleatoriamente por el texto simple *M*. Mediante los componentes aleatorios contenidos *RND1* y *RND2* se consigue que tanto el texto simple *M* como también el texto cifrado *C** sean diferentes en cada proceso de lectura, es decir en cada solicitud.

Ventajosamente, la etiqueta RFID está configurada de tal modo que la etiqueta RFID puede empezar incluso durante la lectura de la demanda con el encriptado. Adicionalmente, los primeros bits o bytes del texto cifrado *C** calculados por la etiqueta RFID, pueden ser ya transmitidos al dispositivo de lectura, mientras los siguientes bits o bytes del texto cifrado *C** son aún calculados por la etiqueta RFID. En otras palabras: la etiqueta RFID está configurada, preferiblemente, para calcular el texto cifrado *C** sucesivamente bit a bit y enviar los bits ya calculados del texto cifrado *C** al dispositivo de lectura como parte del mensaje de autentificación, por lo que no es necesaria ninguna memoria intermedia (registro) y el protocolo de comunicación puede realizarse más rápidamente.

Opcionalmente, en el texto simple *M* se incorpora adicionalmente una firma digital del elemento de identificación de la etiqueta RFID que, preferiblemente, se almacena en la memoria de la etiqueta RFID y puede ser comprobada por el dispositivo de lectura.

De acuerdo con formas de realización preferibles, para el ahorro del tiempo de cálculo el módulo *n* se selecciona como sigue: $n = 1\ (mod 2^{bl \cdot nd})$, donde *nd* es un número entero con $1 \leq nd < d$, *bl* el tamaño de palabra de la unidad de procesador de la etiqueta RFID en bits y *d* la longitud del módulo *n* en tamaños de palabra de unidad de procesador.

En la práctica, para un módulo *n* dado el número *R* se selecciona típicamente como la potencia de dos mayor más próxima, es decir, para un módulo *n* consistente en *k* bits (por ejemplo, 1024 bits) se selecciona $R = 2^k$. Según formas de realización preferibles de la invención se establece que $R = 2^{bl \cdot (d+sd)}$, tal que *bl* es el tamaño de palabra de la unidad de procesador de la etiqueta RFID, *d* es la longitud del módulo *n* en tamaños de palabra de la unidad de procesador y *sd* es un parámetro de seguridad que se selecciona de tal modo que $bl \cdot sd \geq 1$, preferiblemente, $bl \cdot sd \geq 10$ y, lo más preferiblemente, $bl \cdot sd \geq 100$.

Preferiblemente, el dispositivo de lectura es sólo un dispositivo de lectura de múltiples dispositivos de lectura que están conectados entre sí por medio de un sistema de fondo y que pueden acceder a datos almacenados en el sistema de fondo que, respectivamente, está vinculado a una etiqueta RFID respectiva.

De acuerdo con una forma de realización preferible, la etiqueta RFID es una etiqueta UHF según la norma ISO/IEC 18000-63 o la norma EPC Clase 1 Gen 2.

En particular, la presente invención tiene, en particular, las siguientes ventajas. En el encriptado de acuerdo con la invención no se requiere ninguna reducción modular, es decir, ninguna división y no se generan más datos que los correspondientes a la longitud del módulo n. Adicionalmente, la invención proporciona la posibilidad de empezar con el cálculo del texto cifrado *C** antes de que la etiqueta RFID haya recibido todos los datos introducidos en el cálculo y entonces empezar a enviar el resultado de este cálculo al dispositivo de lectura antes de que el cálculo del texto cifrado *C** se haya completado, por lo que la transmisión de datos y el cálculo pueden realizarse paralelamente, pudiendo ahorrarse el tiempo de transacción. Dado que el procedimiento de acuerdo con la invención es un procedimiento de clave pública, únicamente debe almacenarse una clave pública en la etiqueta RFID, de manera que la seguridad del sistema no es puesta en riesgo en el caso de que un atacante obtuviera esta clave pública. Una ventaja adicional de la invención es que para desencriptar el texto cifrado *C** un dispositivo de lectura no tiene por qué estar conectado a un sistema de fondo, puesto que la clave privada requerida para ello puede almacenarse localmente en el dispositivo de lectura. Finalmente, otra ventaja es que la invención puede implementarse en dispositivos de lectura convencionales sin modificaciones de hardware.

Como reconocerá el experto, las configuraciones preferibles definidas en la reivindicaciones dependientes y descritas previamente en el marco del primer aspecto de la invención, pueden implementarse ventajosamente en el marco del segundo aspecto de la invención, en el marco del tercer aspecto de la invención así como en el marco del cuarto aspecto de la invención.

Otras características, ventajas y objetivos de la invención se desprenden de la siguiente descripción detallada de varios ejemplos de realización y alternativas de realización. Se hace referencia a los dibujos en los que se muestra:

la figura 1 muestra una representación esquemática de un sistema para la comunicación segura entre una etiqueta RFID y un dispositivo de lectura según una forma de realización preferible de la invención;

la figura 2 muestra una vista en detalle esquemática de una etiqueta RFID del sistema de la figura 1;

la figura 3 muestra una representación esquemática de una forma de realización preferible de un procedimiento de acuerdo con la invención para la comunicación segura entre una etiqueta RFID y un dispositivo de lectura del sistema de la figura 1; y

la figura 4 muestra un algoritmo para implementar el procedimiento de la figura 3 de acuerdo con la invención.

La figura 1 muestra una representación esquemática de un sistema 10 para la comunicación entre una etiqueta RFID y un dispositivo de lectura según una forma de realización preferible de la invención. El sistema 10 podría tratarse de, por ejemplo, un sistema electrónico dispensador de recibos, en el que una etiqueta RFID representa un recibo electrónico que lleva una persona.

El sistema 10 comprende, a modo de ejemplo, dos etiquetas RFID, concretamente la etiqueta RFID 20a y la etiqueta RFID 20b que, respectivamente, pueden comunicarse por una interfaz de aire con un dispositivo de lectura 30a o un dispositivo de lectura 30b, en cuya zona de lectura o de comunicación se localiza la respectiva etiqueta RFID 20a, 20b. Preferiblemente, las etiquetas RFID 20a, 20b se tratan de etiquetas RFID según la norma ISO/IEC 18000-63 o EPC de Clase 1, Generación 2, que se denominan también etiquetas EPC.

Los dispositivos de lectura 30a, 30b están conectados por medio de una red de comunicación 40 a un sistema de fondo o sistema de parte trasera 50 ("back-end") en el que se almacenan datos vinculados a las etiquetas RFID 20a, 20b, preferiblemente, en un banco de datos. Además de los dispositivos de lectura 30a, 30b, en el sistema 10 representado en la figura 1 incluso pueden estar integrados múltiples dispositivos de lectura adicionales que se comunican con el sistema de fondo 50 por medio de la red de comunicación 40 y que pueden acceder a los datos almacenados ahí. Por claridad, en la figura 1 están representados únicamente dos dispositivos de lectura de RFID 30a, 30b y dos etiquetas RFID, concretamente las etiquetas RFID 20a, 20b. Por supuesto, el sistema 10 representado en la figura 1 está configurado sin embargo de tal modo que además de las etiquetas RFID 20a, 20b en este sistema 10 incluso pueden ser operadas múltiples etiquetas RFID adicionales.

La figura 2 muestra una vista en detalle de la etiqueta RFID 20a a modo de ejemplo del sistema 10 de la figura 1, en la que están representados esquemáticamente los componentes de la etiqueta RFID 20a esenciales para la presente forma de realización preferible de la invención. La etiqueta RFID 20a, cuya estructura puede ser, pero no debe ser, idéntica a la estructura de la etiqueta RFID 20b, comprende una instalación de antena 22 externa o interna para la respectiva comunicación a través de la interfaz de aire con los dispositivos de lectura 30a, 30b del sistema 10 de la figura 1. La instalación de antena 22 se comunica por medio de una interfaz de entrada/salida 24 ("input/output") con una unidad de procesador 25 que puede acceder a una memoria 26 de la etiqueta RFID 20a para almacenar y leer datos.

En la memoria 26 de la etiqueta RFID 20a representada en la figura 2, que se trata de, preferiblemente, una ROM y/o EEPROM (memoria "flash"), se almacenan o pueden almacenarse los datos que se utilizan para la comunicación preferible, segura de acuerdo con la invención y descrita a continuación en detalle, de la etiqueta RFID 20a con uno de los dispositivos de lectura 30a, 30b. En particular, en la memoria 26 de la etiqueta RFID 20a se almacena al menos un elemento de identificación que hace posible una identificación inequívoca de la etiqueta RFID 20a y/o del objeto provisto con la etiqueta RFID 20a. El elemento de identificación almacenado en la memoria 26 puede tratarse de, por ejemplo, un elemento TID ("Tag Identifier") o un elemento UII ("Unique Item Identifier"), preferiblemente, el EPC ("Electronic Product Code") conocido para el experto a partir de la norma EPC. Como puede observarse en la figura 2, en la memoria 26 de la etiqueta RFID 20a están depositadas adicionalmente una clave *n* abierta así como, preferiblemente, una firma digital del elemento de identificación almacenado en la memoria 26, por ejemplo, la firma digital del elemento UII que en la figura 2 se indica como SIG(UII), cuyo propósito se explica con más detalle a continuación en conexión con la figura 3.

Preferiblemente, la etiqueta RFID 20a comprende adicionalmente un generador de números aleatorios 28 (RND) para la generación de números aleatorios que se utilizan para la comunicación segura entre la etiqueta RFID 20a y uno de los dispositivos de lectura 30a, 30b, como se describe en detalle a continuación en conexión con la figura 3. Aunque en la figura 2 el generador de números aleatorios 28 está representado como una unidad separada, el experto en la materia reconocerá que el generador de números aleatorios 28 también podría ser una parte de la unidad de procesador 25 o que podría implementarse como un módulo de software de la unidad de procesador 25. Igualmente, la memoria 26 podría estar configurada como parte de la unidad de procesador 25.

Además del acceso a la memoria 26 de la etiqueta RFID 20a así como de la comunicación interna con la interfaz de entrada/salida 24 y del generador de números aleatorios 28, por ejemplo, por medio de un sistema de bus, la unidad de procesador 25 de la etiqueta RFID 20a está, preferiblemente, adicionalmente configurada para realizar o promover las etapas descritas a continuación en conexión con la figura 3 en lo que respecta a la etiqueta RFID 20a, con objeto de hacer posible una comunicación segura entre la etiqueta RFID 20a y uno de los dispositivos de lectura 30a, 30b.

Tan pronto como un dispositivo de lectura, por ejemplo, el dispositivo de lectura 30a, detecta que una etiqueta RFID, por ejemplo, la etiqueta RFID 20a, se encuentra en su zona de cobertura, el protocolo de comunicación esquematizado en la figura 3 es activado por el dispositivo de lectura 30a. Con ello, primeramente en la etapa S1 de la figura 3 el dispositivo de lectura 30a genera un primer número aleatorio *RND1* (también denominado "Nonce") y envía este primer número aleatorio *RND1* a la etiqueta RFID 20a en la etapa S2 de la figura 3 como demanda en el marco de un procedimiento de demanda-respuesta. Preferiblemente, en respuesta a la recepción del primer número aleatorio *RND1* del dispositivo de lectura 30a, la etiqueta RFID 20a genera en la etapa S3 de la figura 3 un segundo

número aleatorio *RND2*. Así, este segundo número aleatorio *RND2* se genera, preferiblemente, por el generador de números aleatorios 28 de la etiqueta RFID 20a, señaladamente, de forma independiente del primer número aleatorio *RND1*.

Como se describe en detalle a continuación, preferiblemente, tanto el primer número aleatorio *RND1* aportado por el dispositivo de lectura 30a como también el segundo número aleatorio *RND2* aportado por la etiqueta RFID 20a se incorporan en el texto simple *M* a ser encriptado por la etiqueta RFID 20a y a ser transmitido en el dispositivo de lectura 30a. Dado que el texto simple *M* a ser encriptado tiene, por tanto, un elemento aleatorio que cambia en cada proceso de lectura, en cada proceso de lectura se transmite también un texto simple *M* encriptado adicional, es decir otro texto cifrado, desde la etiqueta RFID 20a al dispositivo de lectura 30a. De este modo se puede evitar que un atacante pueda identificar una etiqueta RFID en base a un texto cifrado invariable enviado por esta etiqueta RFID. Además, el primer número aleatorio *RND1* generado por el dispositivo de lectura 30a tiene, como ya se ha mencionado previamente, la función de una demanda en el marco de un procedimiento de demanda-respuesta conocido al experto para autentificar la etiqueta RFID 20a respecto al dispositivo de lectura 30a.

En la etapa S4 de la figura S3 se genera por la etiqueta RFID 20a un texto simple *M* a ser encriptado que hace posible al dispositivo de lectura 30a, que recibe y desencripta el texto simple *M* encriptado, identificar la etiqueta RFID 20a. Para ello, en el texto simple *M* se incorpora, en particular, un elemento de identificación que hace posible una identificación inequívoca de la etiqueta RFID 20a y/o del objeto provisto con la etiqueta RFID 20a. En la forma de realización representada en las figuras, el elemento de identificación se trata del elemento UII almacenado en la memoria 26 de la etiqueta RFID 20a.

Para que el dispositivo de lectura 30a pueda comprobar la autenticidad del elemento UII de la etiqueta RFID 20a, en el texto simple *M* se incorpora adicionalmente, preferiblemente, una firma digital del elemento UII. Preferiblemente, una firma digital del elemento UII se almacena en la memoria 26 de la etiqueta RFID 20a como se indica en la figura 2 con la denominación SIG(UII), para que esta no se deba calcular nuevamente en cada proceso de lectura de la etiqueta RFID 20a. Como es conocido al experto, una firma digital del elemento UII de la etiqueta RFID 20a, puede ser generada, por ejemplo, aplicando una clave privada al elemento UII en el marco de un procedimiento de clave pública ("public-key"). Para comprobar la firma digital del elemento UII, se aplica una clave pública que coincide con la clave privada a la firma digital mediante el dispositivo de lectura 30a.

Preferiblemente, además del elemento UII y la firma digital del elemento UII, en el texto simple *M* se incorpora adicionalmente, como se ha descrito previamente, tanto el primer número aleatorio *RND1* proporcionado por el dispositivo de lectura 30a como también el segundo número aleatorio *RND2* proporcionado por la etiqueta RFID 20a. Preferiblemente, esto se efectúa por medio de una operación de intercalado MIX implementada en la unidad de procesador 25 de la etiqueta RFID 20a que está configurada para intercalar o mezclar entre sí el elemento UII, la firma digital del elemento UII, el primer número aleatorio *RND1* y el segundo número aleatorio *RND2*. En este caso, la mezcla mediante la operación de intercalado MIX puede efectuarse, por ejemplo, a nivel de byte. El resultado de la aplicación de la operación de intercalado MIX en el elemento UII, la firma digital del elemento UII, el primer número aleatorio *RND1* y el segundo número aleatorio *RND2* es el texto simple *M* a ser encriptado. Los bits del texto simple *M* procedentes de los números aleatorios *RND1* y *RND2* pueden ser considerados como bits de relleno ("padding"). En este caso, puede ser ventajoso conseguir, mediante la adecuada selección de la longitud de los números aleatorios *RND1* y *RND2*, que el texto simple *M* tenga la misma longitud que el módulo *n*, por ejemplo, 1024 bits.

Después de que en la etapa S4 de la figura 3 haya sido creado por la etiqueta RFID 20a el texto simple *M* que contiene entre otros el elemento UII, este texto simple *M* es encriptado por la etiqueta RFID 20a en la etapa S5 de la figura 3 del modo siguiente. Como en el procedimiento de Rabin convencional, primeramente, el texto simple *M* es elevado al cuadrado. Para generar el texto cifrado, a continuación sin embargo el resultado de esta operación de elevar al cuadrado no se somete a una operación de módulo con el módulo *n* como en el procedimiento de Rabin convencional, sino que se forma el residuo de Montgomery del texto simple elevado al cuadrado. En general, el residuo de Montgomery ("Montgomery reduction") de un número entero *T* de módulo *n* en relación a un número entero *R* se define como TR^{-1} mod*n*, donde *R* es mayor que el módulo *n, R* y el módulo *n* son números primos relativos (es decir, ggT(*R,n*)=1) y $0 \leq T < nR$ (véase el capítulo 14.3.2 de A. J. Menezes, P.C. van Oorschot, S.C. Vandtone, "Handbook of Applied Cryptography"). En la literatura el número entero *R* se denomina a veces como base de Montgomery.

En el marco de la presente invención, el residuo de Montgomery, calculado por la etiqueta RFID 20a, del cuadrado del texto simple *M* de módulo *n* en relación al número entero *R* se define como texto cifrado *C**, es decir, $C^* = M^2 R^{-1}$ mod*n*, tal que el número entero *R*, como ya se ha mencionado previamente, se elige mayor que el módulo *n*. En la práctica, para un módulo *n* dado, el número *R* se elige típicamente como la potencia de dos mayor más próxima, es decir, para un módulo *n* compuesto por *k* bits (por ejemplo, 1024 bits) se elige $R = 2^k$. Otras opciones preferibles del número R de acuerdo con la presente invención se describen más abajo.

Después de que en la etapa S5 de la figura 3 el texto cifrado $C^* = M^2 R^{-1}$ mod*n* haya sido calculado por la etiqueta RFID 20a, en la etapa S6 de la figura 3 el texto cifrado *C** así calculado se envía como respuesta a la demanda

enviada en la etapa S2 de la figura 3 al dispositivo de lectura 30a. Sin embargo, el experto reconocerá que en vez del texto cifrado $C^* = M^2 R^{-1}$ mod$n$ también podrá ser transmitido al dispositivo de lectura 30a un texto cifrado C^{**} procesado adicionalmente de nuevo por la etiqueta RFID 20a, siempre que la etiqueta RFID 20a y el dispositivo de lectura 30a lo hubieran acordado, como puede recalcular el dispositivo de lectura 30a sobre el texto cifrado $C^* = M^2 R^{-1}$ a partir del texto cifrado C^{**} procesado adicionalmente y transmitido por la etiqueta RFID 20a.

En la etapa S7 de la figura 3, primeramente, el texto cifrado C^* transmitido por la etiqueta RFID 20 en la etapa S6, es multiplicado por R y, a continuación, realizada la operación de módulo con el módulo n, es decir, C^*R mod$n$. Una vez establecida para C^* la expresión descrita en conexión con la etapa S5 de la figura 3, se obtiene: $C^* R$ mod$n = M^2 R^{-} R$ mod$n = M^2$mod$n$. Como reconoce el experto, la última expresión M^2 mod$n$ es el texto cifrado del conocido procedimiento de Rabin que se denomina aquí como texto cifrado C. En otras palabras: En la etapa S7 de la figura 3 se obtiene el conocido texto cifrado $C = M^2$ mod n a partir del conocido procedimiento de Rabin, siendo multiplicado por R el texto cifrado C^* enviado por la etiqueta RFID 20 y, a continuación, realizada la operación de módulo con el módulo n.

Como en el caso del clásico procedimiento de Rabin, entonces en la etapa S8 de la figura 3 mediante el dispositivo de lectura 30a puede determinarse el texto simple M generado por la etiqueta RFID 20a originalmente en la etapa S4, siendo calculada la raíz cuadrada del texto cifrado C de módulo n determinada en la etapa S7. Como se ha descrito ya previamente, para ello puede aprovecharse el teorema chino del resto (CRT) utilizando la clave privada en la forma de los números primos p y q disponible para el dispositivo de lectura 30a, con objeto de calcular las cuatro raíces cuadradas del texto cifrado C. Preferiblemente, una marcación apropiada permite al dispositivo de lectura 30a determinar inequívocamente cuál de las cuatro raíces cuadradas del texto cifrado C es el texto simple M generado originalmente por la etiqueta RFID 20a. Por ejemplo, el primer número aleatorio *RND1* transmitido por el lector 30a puede usarse para seleccionar la raíz cuadrada correcta, es decir, el texto simple M correcto.

Como se ha descrito previamente, el texto simple M se genera en la etapa S4 de la figura 3 al realizarse la operación de intercalado MIX. Como reconoce el experto, por parte del dispositivo de lectura 30a esta operación de intercalado debe hacerse retroactivamente o invertirse, con objeto de que el elemento UII de la etiqueta RFID 20a, la firma digital SIG(UII) del elemento UII, el primer número aleatorio *RND1* y el segundo número aleatorio *RND2* puedan extraerse del texto simple M. Esta inversión de la operación de intercalado MIX y la extracción de la información contenida en el texto simple M se efectúa, preferiblemente, en la etapa S9 de la figura 3. Por supuesto, entre la etiqueta RFID 20a y el dispositivo de lectura 30a debe haberse acordado qué operación de intercalado se utiliza en la etapa S4 de la figura 3, con objeto de poder aplicar la función de inversión para ello en la etapa S9 de la figura 3.

Tras la realización exitosa de la etapa S9 de la figura 3 quedan disponibles para el dispositivo de lectura 30a el elemento UII de la etiqueta RFID 20a, la firma digital del elemento UII, el primer número aleatorio *RND1* y el segundo número aleatorio *RND2*. En base a estos elementos disponibles, el dispositivo de lectura 30a puede identificar y autentificar la etiqueta RFID 20a. Preferiblemente, en la etapa S10 de la figura 3 se comprueba adicionalmente la integridad del elemento UII de la etiqueta RFID 20a por el dispositivo de lectura 30a, comprobando el dispositivo de lectura 30a la firma digital del elemento UII. Es concebible que para ello el dispositivo de lectura 30a acceda al sistema de fondo 50 para, en base al elemento UII de la etiqueta RFID 20a, encontrar una clave pública que se corresponda con la clave privada con la que la firma digital del elemento UII de la etiqueta RFID 20a fue creada originalmente.

Haciendo referencia a la figura 4 a continuación se describe una implementación preferible del cálculo del texto cifrado C^* de acuerdo con la invención, es decir, del encriptado del texto simple M, mediante la etiqueta RFID 20a, cuyo proceso puede dividirse básicamente en tres partes.

En una primera parte del encriptado, el texto simple M se procesa sucesivamente desde el byte de orden inferior al byte de orden superior. Si la operación de intercalado MIX está configurada para distribuir el primer número aleatorio *RND1* del dispositivo de lectura 30a uniformemente en el texto simple M, tras la recepción del primer byte del número aleatorio *RND1* puede empezarse ya con la primera parte del encriptado y se calcula mientras estén disponibles bytes del texto simple M. Tras la recepción del siguiente byte del número aleatorio *RND1* del dispositivo de lectura 30a el encriptado continúa calculándose hasta que todo el texto simple M haya sido encriptado.

En una segunda parte del encriptado se efectúa un número acordado en el sistema de etapas de Montgomery adicionales, es decir, el número R se selecciona correspondientemente mayor que la potencia de dos más próxima disponible mayor que el módulo n. La razón para esta medida es que reduce la probabilidad de que el resultado final del encriptado sea mayor que el módulo n (lo que naturalmente un atacante podría reconocer y usar para causar un ataque de canal lateral). La probabilidad de tal desbordamiento se limita a $2^{-bl \cdot sd}$, donde bl indica la longitud de bit de la operación de grandes números utilizada y sd el número redondeado adicional (= cifras) en la segunda parte del encriptado. Es recomendable elegir estos números de modo que cumplan, preferiblemente, $bl \cdot sd \geq 10$ y, lo más preferiblemente, $bl \cdot sd \geq 100$, prescindiendo para ello de una comprobación explícita de desbordamiento. En cualquier caso, si accidentalmente ocurriera un desbordamiento, el resultado sin reducción modular puede ser enviado al dispositivo de lectura 30a.

Finalmente, en la tercera parte del encriptado se generan sucesivamente los datos de salida encriptados que seguidamente pueden ser enviados al dispositivo de lectura 30a solapadamente con el cálculo completado. Esto es especialmente ventajoso ya que debido a la longitud del texto cifrado C^* (con la longitud del módulo n usual y necesaria de 1024 bits resulta un texto cifrado de 128 bytes) los datos en cualquier caso no pueden ser enviados en una sola etapa de transmisión (bloque de datos). Los dispositivos de lectura de RFID UHF disponibles comercialmente (según ISO/IEC 18000-63) no están configurados para transmitir bloques de datos más grandes sino que limitan el tamaño de bloque de acuerdo con el estado de la técnica de 2 a 16 bytes. Mediante la transmisión por partes de los datos del texto cifrado C^* (denominado encadenamiento, "chaining") los datos se transmiten por partes de forma secuencial. El solapamiento resultante de ello entre el cálculo y la transmisión puede ser utilizado de forma muy ventajosa a efectos de que incluso una vez recibidos los primeros datos puede empezarse con el cálculo paralelamente a la transmisión de datos.

La figura 4 muestra un algoritmo ("cuadrado de Montgomery") para calcular el texto cifrado C^*, es decir, para encriptar el texto simple M, mediante la etiqueta RFID 20a. Para la siguiente descripción de este algoritmo, son de ayuda las siguientes definiciones. Se asume que la unidad de procesador 25 de la etiqueta RFID 20a tiene un tamaño de palabra de bl bits. En este caso, la unidad de procesador 25 de la etiqueta RFID 20a está configurada de tal modo que dos palabras de tamaño bl bits pueden multiplicarse entre sí, tal que el resultado puede ser de $2 \cdot bl$ bits de tamaño. De manera no limitativa se asume adicionalmente que el módulo n tiene como máximo una longitud de d palabras y por tanto $d \cdot bl$ bits. Según una forma de realización preferible de la invención un parámetro de seguridad sd se selecciona de tal modo que la probabilidad de desbordamiento descrita previamente es del orden de magnitud de $2^{-bl \cdot sd}$. Como reconoce el experto, un valor mayor de sd requiere de un tiempo de cálculo mayor. Se establece de forma no limitativa que $R = 2^{bl \cdot (d+sd)}$. Como ya se ha descrito previamente, R o el parámetro de seguridad sd deberían ser elegidos, preferiblemente, de tal modo que cumplan, preferiblemente, $bl \cdot sd \geq 10$ y, lo más preferiblemente, $bl \cdot sd \geq 100$.

Para un texto simple M que se trata de un número con $0 \leq M < n$, el texto cifrado C^* puede ser calculado con $C^* = M^2 \cdot R^{-1} \bmod n$ por medio de los dos pasos siguientes:

1. Calcular un a que cumpla: $a = -M^2 / n \bmod R$, $0 \leq a < R$.
2. Establecer $C^* = (M^2 + a \cdot n)/ R$

Aquí la división es ejecutable en la segunda etapa sin resto. Dado que $0 \leq M < n$, puede asumirse que con M seleccionado aleatoriamente el valor a está distribuido también uniformemente en el intervalo [0, … , R-1]. Por tanto la probabilidad de un desbordamiento de C^* (es decir que se cumpla $C^* \geq n$) es como máximo igual a n/R y por tanto como máximo igual a $2^{-bl \cdot sd}$.

Para un número entero x, sea $(x_0, x_1, ..., x_i, ..., x_{v-1})$ la representación de x para la base 2^{bl}, es decir, que cumple que $x = \sum_{i=0}^{v-1} 2^{bl \cdot i} \cdot x_i$, $0 \leq x_i < 2^{bl}$. Sean $(M_0, ..., M_{d-1})$, $(n_0, ..., n_{d-1})$, $(a_0, ..., a_{d+sd-1})$, y $(C^*_0, ..., C^*_{d-1})$ las representaciones de M, n, a y C^* para la base 2^{bl}. Adicionalmente, sea n_{inv} el número entero determinado inequívocamente mediante $n \cdot n_{inv} = -1 (mod\ 2^{bl})$ y $0 \leq n_{inv} < 2^{bl}$. Entonces a y C^* pueden calcularse según el algoritmo de "cuadrado de Montgomery" representado en la figura 4, teniendo en cuenta que las cifras binarias $C^*_0, ..., C^*_{d-1}$ de C^* se designan en el algoritmo representado en la figura 4 como C_{i-s-sd}.

En relación con el algoritmo de "cuadrado de Montgomery" representado en la figura 4, el experto reconocerá lo siguiente.

Tras el paso i de la iteración principal se cumple $a = -M^2/n (mod 2^{bl \cdot \min(i, d+sd)})$ y en el caso de $i > d + sd$ además se cumple $C^* = (M^2 + a \cdot n)/R\ (mod\ 2^{bl \cdot (i-d-sd)})$. Para cualquier posición i de la iteración principal sólo se requieren los primeros valores de entrada de i M_0, …, M_{i-1}, de manera que este paso puede realizarse incluso después de presentarse los primeros valores de entrada de i. El valor de salida de posición i puede entonces ya extraerse después de $i+s+sd$ pasos de la iteración principal. Por tanto, el solapamiento de entrada, procesamiento y salida descritos anteriormente es directamente posible de acuerdo con la invención.

Del valor intermedio a, en el paso de posición i de la iteración principal se requieren sólo los puntos $a_i, …, a_{i-d+1}$, de manera que d palabras de bl bits cada una son suficientes para almacenar la parte requerida exactamente de a.

El algoritmo requiere en total como máximo $(d + 1)\ (3d/2 + sd)$ multiplicaciones.

De acuerdo con una forma de realización preferible de la invención para ahorrar tiempo de cálculo el módulo n se selecciona como sigue: $n = 1 (mod 2^{bl \cdot nd})$, donde nd es un número entero con $1 \leq nd < d$. En este caso se cumple $n_{inv} = 2^{bl} - 1$. La multiplicación con $n_{inv} = 2^{bl} - 1\ (mod\ 2^{bl})$ entonces es una simple negación. Aparte del último punto n_0, los puntos de valor más bajo n_{nd-1}, …, n_1 de n entonces son iguales a cero, de manera que en comparación con el algoritmo descrito anteriormente del "cuadrado de Montgomery" pueden ahorrarse $nl \cdot (d+sd)$ multiplicaciones. Si se selecciona, por ejemplo, $nl = d/2$, entonces el número de multiplicación es del orden de magnitud de $d(d+sd)$. Esto ahorra aproximadamente un tercio de las multiplicaciones en comparación con el algoritmo descrito

anteriormente del “cuadrado de Montgomery”. Los números primos *p, q* con $log\ p \approx log\ q$, $2^{bl \cdot d-1} < n = p \cdot q < 2^{bl \cdot d}$ y $n = p \cdot q = 1\ (\mathrm{mod} 2^{bl \cdot d/2})$ pueden obtenerse fácilmente. La condición establecida para n significa que los bits de la mitad inferior (excepto el último bit) en la representación binaria de *n* son iguales a cero. De acuerdo con el estado de la técnica conocido hoy, esto no supone ninguna limitación para la seguridad del procedimiento. El algoritmo conocido más rápido actualmente para factorizar cualquier número *n* es la criba general del cuerpo de números (“General Number Field Sieve”, GNFS). El único algoritmo conocido claramente más rápido que, bajo ciertas circunstancias, puede factorizar un número $n = p \cdot q$, con $log\ p \approx log\ q$ para números primos *p, q*, es la criba especial del cuerpo de números (“Special Number Field Sieve”, SNFS). Para un $n = p \cdot q$ aleatoriamente elegido, en el que la mitad inferior de los bits son nulos (excepto el último bit), sin embargo no se puede aplicar el SNSF.

Como el experto en la materia reconocerá, las etapas individuales del protocolo de comunicación representado en la figura 3 no tienen que realizarse necesariamente en la secuencia de tiempo mostrada. Es obvio que esto no sólo se requiere cuando los resultados de una etapa representen los datos de entrada de una etapa adicional. Además, el experto reconocerá que aunque previamente se han descrito formas de realización preferibles de la invención haciendo referencia a una etiqueta RFID, que se trata de, preferiblemente, una etiqueta de UHF según la ISO/IEC 18000-63 o EPC Clase 1 Gen 2, la invención puede ser utilizada también ventajosamente con otros tipos de soportes de datos portátiles limitados a recursos, que deban ser autentificados a través de la interfaz de aire respecto a un dispositivo de lectura tal como, por ejemplo, tarjetas inteligentes sin contacto, “tokens” y similares.

REIVINDICACIONES

1. Procedimiento para la comunicación segura entre una etiqueta RFID (20a, 20b) y un dispositivo de lectura (30a, 30b), comprendiendo el procedimiento las siguientes etapas que se realizan en la etiqueta RFID (20a, 20b):

- recibir del dispositivo de lectura un número aleatorio RND1 como demanda en el marco de un procedimiento de demanda-respuesta;
- en respuesta a la recepción del número aleatorio RND1, encriptar un texto simple *M*, en el que se incorporan un elemento de identificación (UII) de la etiqueta RFID (20a, 20b) o de un objeto provisto con el mismo así como el número aleatorio RND1, para calcular un texto cifrado *C**, calculando el residuo de Montgomery del cuadrado del texto simple *M* de módulo *n* con respecto a la base *R* de Montgomery, es decir, $C^* = M^2 R^{-1} \bmod n$; y
- enviar un mensaje de autentificación al dispositivo de lectura (30a, 30b), conteniendo el mensaje de autentificación el texto cifrado *C**,

tal que el módulo $n = p \cdot q$ es la clave pública del dispositivo de lectura (30a, 30b), los números primos *p, q* son la clave privada del dispositivo de lectura (30a, 30b) y la base de Montgomery *R* es un número entero que es mayor que el módulo *n*.

2. Procedimiento para la comunicación segura entre una etiqueta RFID (20a, 20b) y un dispositivo de lectura (30a, 30b), comprendiendo el procedimiento las siguientes etapas que se realizan en el dispositivo de lectura (30a, 30b):

- transmitir un número aleatorio RND1 como una demanda en el marco de un procedimiento de demanda-respuesta a la etiqueta RFID (20a, 20b)
- recibir de la etiqueta RFID (20a, 20b) un mensaje de autentificación que contiene un texto simple *M* encriptado, en el que se ha incorporado un elemento de identificación (UII) de la etiqueta RFID (20a, 20b) o de un objeto provisto con el mismo así como el número RND1 y;
- desencriptar el texto simple *M* encriptado, comprendiendo la etapa de desencriptado multiplicar el texto simple *M* encriptado por una base de Montgomery *R* y subsiguientemente realizar la operación de módulo con el módulo *n*;

tal que el módulo $n = p \cdot q$ es la clave pública del dispositivo de lectura (30a, 30b), los números primos *p, q* son la clave privada del dispositivo de lectura (30a, 30b) y la base de Montgomery *R* es un número entero que es mayor que el módulo *n*.

3. Procedimiento, según la reivindicación 1, tal que en el texto simple M se incorpora adicionalmente un segundo número aleatorio *RND2* generado por la etiqueta RFID (20a, 20b).

4. Procedimiento, según la reivindicación 3, tal que los datos incorporados en el texto simple *M* son mezclados por medio de una operación de intercalado para distribuir los datos aleatorios que proceden del dispositivo de lectura (30a, 30b) y de la etiqueta RFID (20a, 20b) aleatoriamente en el texto simple *M*.

5. Procedimiento, según la reivindicación 3, tal que la etiqueta RFID (20a, 20b) está configurada de tal modo que el texto cifrado *C** se calcula sucesivamente bit a bit y los bits ya calculados del texto cifrado *C** se transmiten al dispositivo de lectura (30a, 30b) como parte del mensaje de autentificación, de manera que la etiqueta RFID (20a, 20b) puede empezar con el encriptado aún durante la lectura de la demanda en la forma del primer número aleatorio *RND1* y los primeros bytes del texto cifrado *C** calculado pueden ser ya emitidos al dispositivo de lectura (30a, 30b) mientras los bytes subsiguientes del texto cifrado *C** están siendo todavía calculados.

6. Procedimiento, según la reivindicación 1 o 2, tal que en el texto simple *M* se incorpora adicionalmente una firma digital (SIG(UII)) del elemento de identificación (UII) de la etiqueta RFID (20a, 20b), que se almacena, preferiblemente, en la unidad de almacenamiento (26) de la etiqueta RFID (20a, 20b) y puede ser comprobada por el dispositivo de lectura (30a, 30b).

7. Procedimiento, según la reivindicación 1 o 2, tal que el módulo *n* se elige para ahorrar tiempo de cálculo como sigue: $n = 1 \pmod{2^{bl \cdot nd}}$, donde *nd* es un número entero con $1 \leq nd < d$, *bl* es el tamaño de palabra de la unidad de procesador (25) de la etiqueta RFID (20a, 20b) y *d* es la longitud del módulo *n* en tamaño de palabra de la unidad de procesador (25).

8. Procedimiento, según la reivindicación 1 o 2, tal que la base de Montgomery *R* se elige para un módulo *n* dado como sigue: $R = 2^{bl \cdot (d+sd)}$, donde *bl* es el tamaño de palabra de la unidad de procesador (25) de la etiqueta RFID (20a, 20b), *d* es la longitud del módulo *n* en tamaños de palabra de la unidad de procesador (25) y *sd* es un parámetro de seguridad que se elige de tal modo que cumple que $bl \cdot sd \geq 1$, preferiblemente, $bl \cdot sd \geq 10$ y lo más preferible $bl \cdot sd \geq 100$.

9. Etiqueta RFID (20a, 20b) para la comunicación segura con un dispositivo de lectura (30a, 30b), tal que la etiqueta RFID (20a, 20b) comprende una unidad de procesador (25) y una unidad de almacenamiento (26) en las que se almacena un elemento de identificación (UII) y tal que la unidad de procesador (25) está configurada para:

- recibir del dispositivo de lectura un número aleatorio RND1 como demanda en el marco de un procedimiento demanda-respuesta;
- en respuesta a la recepción del número aleatorio RND1, encriptar un texto simple *M*, en el que se incorporan un elemento de identificación (UII) de la etiqueta RFID (20a, 20b) o de un objeto provisto con el mismo así como el número RND1, para calcular un texto cifrado *C**, calculando el residuo de Montgomery del cuadrado del texto simple *M* de módulo *n* con respecto a la base *R* de Montgomery, es decir, $C^* = M^2 R^{-1} \bmod n$; y
- enviar un mensaje de autentificación al dispositivo de lectura (30a, 30b), conteniendo el mensaje de autentificación el texto cifrado *C**, tal que el módulo $n = p \cdot q$ es la clave pública del dispositivo de lectura (30a, 30b), los números primos *p, q* son la clave privada del dispositivo de lectura (30a, 30b) y la base de Montgomery *R* es un número entero que es mayor que el módulo n.

10. Dispositivo de lectura (30a, 30b) para la comunicación segura con una etiqueta RFID (20a, 20b), tal que el dispositivo de lectura (30a, 30b) comprende una unidad de procesador que está configurada para transmitir un número aleatorio RND1 como una respuesta en el marco de un procedimiento de demanda-respuesta a la etiqueta RFID y recibir de la etiqueta RFID (20a, 20b) un mensaje de autentificación que contiene un texto simple *M* encriptado, en el que se ha incorporado un elemento de identificación (UII) de la etiqueta RFID (20a, 20b) o de un objeto provisto con el mismo así como el número RND1 generado por el dispositivo de lectura y desencriptar el texto simple *M* encriptado, tal que en el desencriptado el texto simple *M* encriptado se multiplica por una base de Montgomery *R* y subsiguientemente se realiza la operación de módulo con el módulo *n*; tal que el módulo $n = p \cdot q$ es la clave pública del dispositivo de lectura (30a, 30b), los números primos *p, q* son la clave privada del dispositivo de lectura (30a, 30b) y la base de Montgomery *R* es un número entero que es mayor que el módulo *n*.

11. Sistema (10) para la comunicación segura con al menos una etiqueta RFID (20a, 20b), según la reivindicación 9 y al menos un dispositivo de lectura (30a, 30b), según la reivindicación 10.

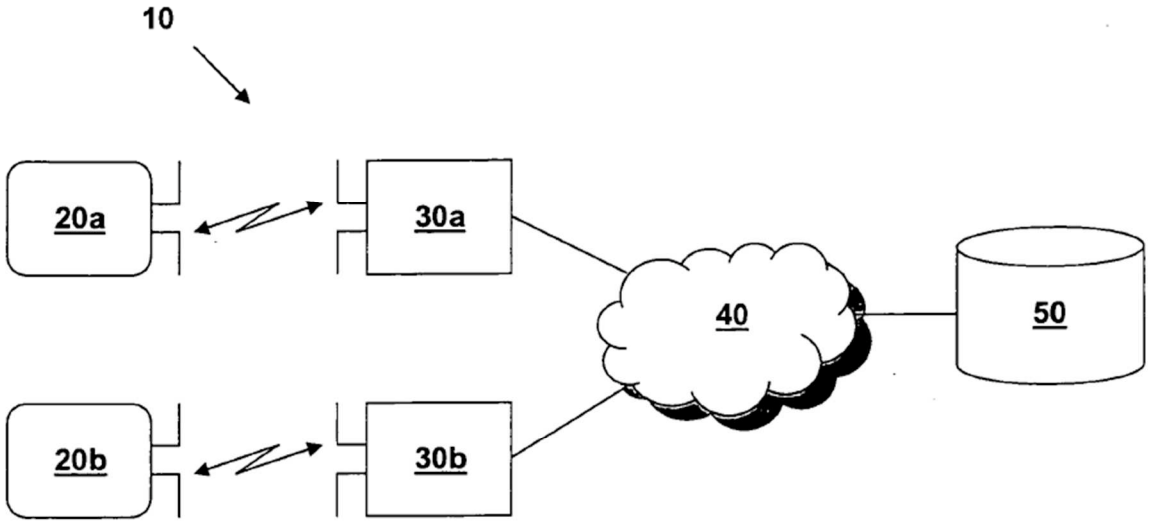

Fig. 1

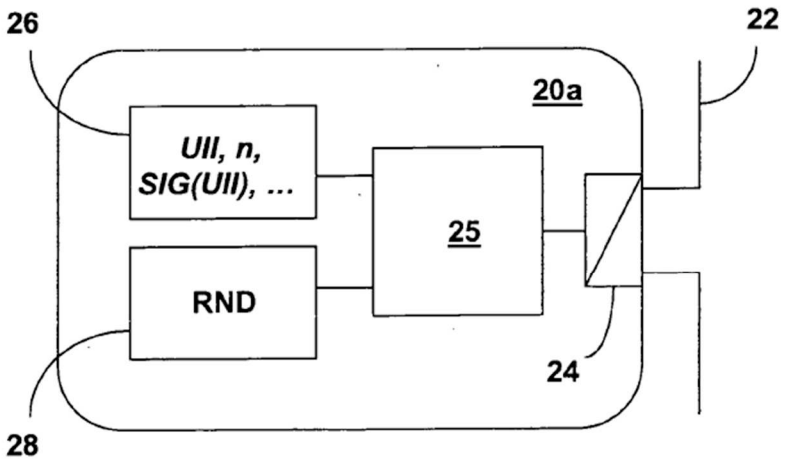

Fig. 2

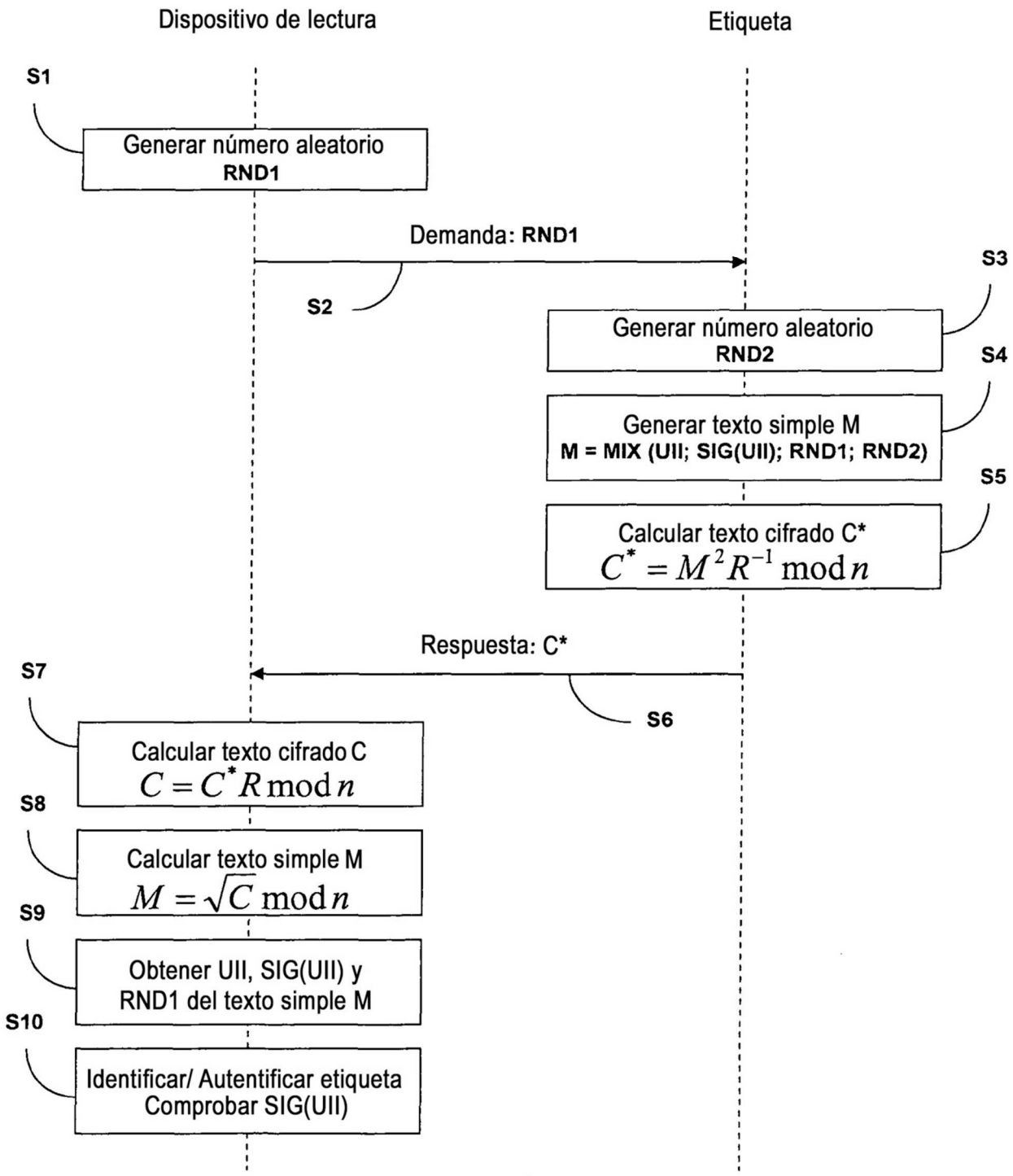
Dispositivo de lectura
Etiqueta
S1
Generar número aleatorio
RND1
Demanda: RND1
S2
S3
Generar número aleatorio
RND2
S4
Generar texto simple M
M = MIX (UII; SIG(UII); RND1; RND2)
S5
Calcular texto cifrado C*
$C^* = M^2 R^{-1} \bmod n$
Respuesta: C*
S6
S7
Calcular texto cifrado C
$C = C^* R \bmod n$
S8
Calcular texto simple M
$M = \sqrt{C} \bmod n$
S9
Obtener UII, SIG(UII) y
RND1 del texto simple M
S10
Identificar/ Autentificar etiqueta
Comprobar SIG(UII)

Fig. 3

```
Algoritmo Cuadrado de Montgomery:
    acc = 0
    i = 0
    while (i < 2 * d + sd):
        // Elevar al cuadrado m
        j = max(0, i + 1 - d);  k = i - j
        acc1 = 0
        while k > j:
            acc1 = acc1 + m_j * m_k
            j = j + 1 ;  k = k - 1
        acc = acc + 2 * acc1
        if j == k:
            acc = acc + m_j * m_j
        // Reducción de Montgomery
        if i < d + sd:
            k = min(i, d - 1);  j = i - k
            while k > 0:
                acc =  acc + a_j * n_k
                j = j + 1;  k = k - 1
            a_i = (acc * n_inv) mod 2^bl
            acc = acc + a_i * n_j
        else:
            k = max(0, i - d - sd + 1);  j = i - k
            while k < d:
                acc = acc +  a_j * n_k
                j = j - 1;  k = k + 1
            c_i-d-sd = acc mod 2^bl
        acc = acc / 2^bl
        i = i + 1
    stop
```

Fig. 4