(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 358 918**

(51) Int. Cl.:
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06726153 .7**
(96) Fecha de presentación : **30.03.2006**
(97) Número de publicación de la solicitud: **1869823**
(97) Fecha de publicación de la solicitud: **26.12.2007**

(54) Título: **Procedimiento de comunicación entre un lector y un marcador de identificación sin cable, lector y marcador asociados.**

(30) Prioridad: **15.04.2005 FR 05 03821**

(45) Fecha de publicación de la mención BOPI:
16.05.2011

(45) Fecha de la publicación del folleto de la patente:
16.05.2011

(73) Titular/es: **MORPHO**
27, rue Leblanc
75015 Paris, FR

(72) Inventor/es: **Chabanne, Hervé**

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procedimiento de comunicación entre un lector y un marcador de identificación sin cable, lector y marcador asociados.

La presente invención se refiere a la comunicación entre un lector y un marcador de identificación sin hilo o inalámbrico.

Se entenderá por marcador de identificación sin hilo cualquier entidad sin hilo que comprenda un componente de dimensiones reducidas, constituido por un circuito y por medios de emisión/recepción. El marcador puede ser, por ejemplo, una etiqueta de identificación por radio frecuencia RFID ("Radio-Frequency IDentification"), cuyos medios de emisión/recepción comprendan una radio-antena. Se puede tratar igualmente de una tarjeta de pulgar sin contacto. Se puede considerar también un marcador del tipo de infrarrojos.

Tales marcadores sin hilo son conocidos y capaces de transmitir, a la petición de un lector de identificación sin hilo, un único identificador de una centena de bits a algunos metros de distancia.

Algunos de estos marcadores, como las etiquetas RFID, por ejemplo, tienen pequeñas capacidades de cálculo. Ello impide contemplar el asegurar las transmisiones con un lector correspondiente, por medio de las soluciones tradicionales a base de aritmética.

Sin embargo, no se puede concebir y generalizar un uso de estos marcadores más que si el mismo prevé mecanismos de seguridad suficientemente fiables.

A este fin, se ha propuesto explotar el ruido inherente al canal de comunicación entre un marcador y un lector correspondiente para asegurar la confidencialidad de los intercambios en presencia de un atacante pasivo, es decir, de un atacante que se contente con escuchar los intercambios sin interactuar con el marcador o el lector.

No obstante, incluso si el protocolo propuesto a este fin tiene el mérito de ser simple en su puesta en práctica, aquel está basado en la hipótesis de que los errores a los cuales se enfrenta el atacante durante su escucha de los intercambios son independientes de los introducidos por el canal de comunicación ruidoso entre el marcador y el lector.

En la práctica, esta hipótesis no siempre se verifica. En particular, el atacante podría disponer de capacidades de escucha suficientes para determinar por correlación, a partir de los datos que él reciba, los datos recibidos por el marcador o el lector.

Un objetivo de la presente invención es el de ofrecer un nivel de seguridad más satisfactorio entre un lector y un marcador sin hilo.

La invención propone de ese modo un procedimiento de comunicación entre un lector de identificación sin hilo y un marcador de identificación sin hilo por intermedio de un canal ruidoso, que comprende:

/a/ la transmisión de una primera cadena numérica o digital desde el lector hacia el marcador;
/b/ la recepción, en el marcador, de una segunda cadena numérica o digital correspondiente, en la primera cadena numérica, a los errores introducidos por el canal ruidoso cercano;
/c/ la introducción de errores artificiales en una al menos de la primera y la segunda cadenas numéricas;
/d/ una fase de destilación de ventaja en la cual se determina, en el lector, una nueva primera cadena numérica a partir de la primera cadena numérica y se determine, en el marcador, una nueva segunda cadena numérica, de manera que se tome la ventaja sobre un eventual atacante pasivo;
/e) una fase de reconciliación de información en la cual se aplica un protocolo de corrección de errores a la nueva primera y a la nueva segunda cadenas numéricas, de manera que, a la salida de la etapa /e/, la nueva primera y la nueva segunda cadenas numéricas sean idénticas con un nivel de probabilidad predeterminado; y
/f/ una fase de amplificación de secreto en la cual se aplica una función de cálculo de clave (hashing) a la nueva primera y a la nueva segunda cadenas numéricas.

La introducción de errores artificiales en la primera y/o la segunda cadenas numéricas, además de los errores naturales vinculados al ruido introducido por el canal de comunicación ruidoso, permite atenuar, incluso suprimir, la eventual correlación de los errores que impactan al lector o al marcador, por una parte, y al atacante que escucha el canal ruidoso, por otra parte. Se complica así la tarea del atacante, el cual ya no es capaz de deducir, de las informaciones que él adquiere, las informaciones recibidas por el marcador.

Una tal introducción de errores artificiales, que puede consistir en la modificación de algunos valores numéricos, por ejemplo elegidos de manera aleatoria, de la primera y/o la segunda cadenas numéricas, es además de puesta en práctica sencilla.

Las etapas del procedimiento son ventajosamente puestas en práctica para que la nueva primera y la nueva segunda cadenas numéricas sean idénticas con un nivel de probabilidad predeterminad, de preferencia próximo al 100%. De ese modo, la función de cálculo de clave suministrará un valor reducido idéntico cuando se aplica a la nueva primera y a la nueva segunda cadenas numéricas.

La etapa /d/ puede ser ventajosamente repetida un número de veces dependiendo del ruido estimado en el canal ruidoso.

La invención propone además un lector de identificación sin hilo apto para comunicar con un marcador de identificación sin hilo por intermedio de un canal ruidoso, que comprende:

- medios para transmitir una primera cadena numérica hacia el marcador;
- medios para introducir errores artificiales en la primera cadena numérica;
- medios para determinar una nueva primera cadena numérica a partir de la primera cadena numérica, de manera que se tome la ventaja sobre un eventual atacante pasivo;
- medios para aplicar un protocolo de corrección de errores a la nueva primera cadena numérica; y
- medios para aplicar una función de cálculo de clave a la nueva cadena numérica.

La invención propone igualmente un marcador de identificación sin hilo apto para comunicar con un lector de identificación sin hilo por intermedio de un canal ruidoso, que comprende:

- medios para recibir una segunda cadena numérica correspondiente en una primera cadena numérica transmitida por el lector, a los errores introducidos por el canal ruidoso cercano;
- medios para introducir errores artificiales en la segunda cadena numérica;
- medios para determinar una nueva segunda cadena numérica a partir de la segunda cadena numérica, de manera que se tome ventaja sobre un eventual atacante pasivo;
- medios para aplicar un protocolo de corrección de errores a la nueva segunda cadena numérica; y
- medios para aplicar una función de cálculo de clave a la nueva segunda cadena numérica.

Otras particularidades y ventajas de la presente invención se desprenderán de la descripción que sigue de ejemplos de realización no limitativos, con referencia a los dibujos anejos, en los cuales:

- la figura 1 es un esquema que muestra de manera simplificada un sistema en el que puede ser puesta en práctica la invención;
- las figuras 2-5 muestran cadenas numéricas simplificadas puestas en práctica en un ejemplo de realización de la invención;
- la figura 6 es un esquema que ilustra de manera simplificada una operación de cálculo de clave puesta en práctica en un ejemplo de realización de la invención.

La figura 1 muestra un lector RFID 1 apto para comunicar con una etiqueta RFID 2. Se observará que podría ser igualmente utilizado en el marco de la invención cualquier otro tipo de marcador sin hilo (tarjeta de pulgar, marcador de infrarrojos, etc.) que tenga capacidades para comunicar con un lector correspondiente.

El lector 1 y la etiqueta 2 son aptos para intercambiar cadenas numéricas, es decir sucesiones de valores numéricos o digitales, por ejemplo binarios, por intermedio de un canal de comunicación de radio 3. El canal 3 es generalmente ruidoso, es decir, que introduce errores en cada transmisión. De ese modo, cuando el lector 1 transmite una cadena numérica por el canal 3, la etiqueta 2 recibe una cadena numérica que difiere más o menos de la cadena numérica transmitida en función del nivel de ruido introducido por el canal 3.

Se supone, por otra parte, que el atacante pasivo 4 intenta adquirir los datos intercambiados entre el lector 1 y la etiqueta 2. A este fin, el atacante 4 escucha el canal 3 y puede efectuar cualquier tipo de operación sobre los datos adquiridos con el fin de hacer fracasar la seguridad puesta en práctica entre el lector 1 y la etiqueta. A título de ejemplo, el atacante 4 puede poner en práctica las mismas operaciones que el lector 1 y la etiqueta 2.

En el ejemplo que se va describir a continuación, se pretende obtener de la etiqueta 2 una información o “clave” sin que el atacante 4 pueda adquirirla él mismo. Esta clave podrá ser utilizada a continuación para poner en práctica mecanismos de seguridad entre el lector 1 y la etiqueta 2.

La figura 2 muestra un ejemplo de cadena numérica X_0 transmitida por el lector 1 con destino a la etiqueta 2 por intermedio del canal 3 ruidoso. Se observará que el ejemplo de cadena numérica elegido comprende un número reducido de bits, es decir, de elementos binarios, para facilitar la comprensión de las operaciones puestas en práctica. En realidad, las cadenas numéricas transmitidas por el lector pueden ser del orden de la decena de millares de bits, por ejemplo.

Debido al ruido presente en el canal 3, la etiqueta 2 recibe una cadena numérica Y_0 en la cual algunos bits son diferentes de los bits correspondientes de X_0. Estas diferencias 5 han sido representadas en la figura 2. Las mismas están en número de cuatro.

Se ha elegido a continuación considerar la cadena numérica Y_0 como la cadena de referencia, es decir que Y_0 se considera, por convención, como no comprendiendo error. Por el contrario, las diferencias entre bits de otras cadenas numéricas y los bits correspondientes de Y_0 son consideradas como errores. Por supuesto, se trata de aquí de una hipótesis. Son igualmente posibles otras elecciones de cadena de referencia, como X_0, por ejemplo.

En cuanto al atacante 4, que escucha el canal 3, recibe una cadena numérica Z_0 que difiere de X_0 debido al ruido introducido por el canal 3. Z_0 difiere también de Y_0, principalmente porque el atacante puede estar situado en un lugar ligeramente diferente de la etiqueta 2 y porque las características del canal 3 pueden variar en el tiempo y en el espacio. Los errores contenidos en Z_0 pueden ser independientes o estar relativamente poco correlacionados con los contenidos en Y_0.

De ese modo, se constata en el ejemplo ilustrado en la figura 2 que Z_0 presenta cinco diferencias con Y_0. Cuatro de estas diferencias (diferencias 6) son las mismas que las diferencias 5 entre X_0 y la cadena de referencia Y_0, mientras que la quinta (diferencia 7) es un error introducido por el canal 3 entre el lector 1 y el atacante 4.

Según la invención, el lector 1 calcula una nueva cadena numérica X'_0, en sustitución de X_0, modificando ciertos bits de X_0. Esta modificación consiste así en introducir errores artificiales, por ejemplo de manera aleatoria, en X_0. Estos errores artificiales no dependen del cana ruidoso 3. Los mismos se superponen a los errores “naturales” introducidos por el canal ruidoso 3. La conjunción de los errores naturales y artificiales entre el lector 1 y la etiqueta 2 impide así al atacante, incluso si éste posee capacidades de escucha suficientes, descubrir una correlación cualquiera entre estos errores y los errores que él mismo sufre escuchando el canal ruidoso 3. En efecto, incluso si los errores naturales introducidos por el canal 3 al nivel de la etiqueta 2 y del atacante 4 están correlacionados, la introducción adicional de errores artificiales por el lector 1 atenúa, incluso suprime, esta correlación.

Como variante, los errores artificiales pueden ser introducidos por la etiqueta 2 en la cadena numérica Y_0. Aquellos pueden ser introducidos también a la vez en las dos cadenas numéricas X_0 e Y_0 por el lector 1 y la etiqueta 2, respectivamente.

En el ejemplo ilustrado en la figura 3 han sido introducidos por el lector 1 tres errores artificiales en la cadena numérica X_0, transformando los valores “1” en “0”, e inversamente. Debido a ello, la cadena modificada X'_0 comprende tres diferencias con X_0 (diferencias 8).

Las otras operaciones descritas aquí son conocidas.

Se efectúa en primer lugar una fase de destilación de ventaja en la cual se aumenta la probabilidad de que el atacante 4 tenga una cadena numérica que presente un mayor número de diferencias con X'_0 que la cadena numérica obtenida al nivel de la etiqueta 2. Dicho de otro modo, esta fase permite a una pareja lector 1 – etiqueta 2 tomar ventaja sobre el atacante pasivo. Un ejemplo de operaciones puestas en práctica en una tal fase de destilación de ventaja ha sido divulgado por Martin Gander y Ueli Maurer en el artículo “On the secret-key rate of binary random variables, Proc. 1994 IEEE International Symposium on Information Theory (Abstracts), 1994”, p. 351. Por supuesto, pueden ser puestas en práctica otras operaciones a condición de que estas permitan bien tomar ventaja sobre el atacante pasivo.

En un ejemplo de una tal fase de destilación de ventaja, las cadenas numéricas X'_0 e Y_0 se descomponen en grupos de N valores numéricos, siendo N entero. En el ejemplo ilustrado en la figura 3, los bits de X'_0 e Y_0 están agrupados por parejas (N=2). Después, por cada pareja así identificada, se aplica una “O exclusiva” (XOR) de manera que se obtiene un “1” cuando los bits de la pareja considerada son diferentes y un “0” cuando son idénticos.

Se comparan a continuación los resultados de la O exclusiva con grupos correspondientes (es decir, del mismo rango) de X'_0 e Y_0. Para ello, cada uno del lector 1 y la etiqueta 2 transmite por el canal 3 los resultados de la O exclusiva que ha efectuado.

Se determinan entonces nuevas cadenas numéricas X_1 e Y_1, conservando los primeros valores numéricos de cada grupo de X'_0 e Y_0, respectivamente, para el cual el resultado de la O exclusiva es el mismo que para el grupo correspondiente de la otra cadena numérica (Y_0 ó X'_0). Los otros grupos son ignorados y no son tenidos en cuenta en la constitución de las cadenas numéricas X_1 e Y_1.

En el ejemplo ilustrado en la figura 3 se constatan cinco diferencias entre bits de la O exclusiva efectuada respectivamente sobre X'_0 e Y_0. Algunas de estas diferencias tienen como causa los errores naturales introducidos por el canal 3 (diferencias 9). Otras diferencias se explican por la introducción de errores artificiales en la cadena inicial X_0 (diferencias 10). Se observará que la O exclusiva efectuada sobre el penúltimo par (referencia 11 en la

figura 3) tiene el mismo resultado, a saber un “1”, para X'_0 e Y_0 por el hecho de que cada uno de los dos bits del par en cuestión de X_0 ha sido modificado por el canal ruidoso 3 antes de su recepción por la etiqueta 2.

Las cadenas numéricas X_1 e Y_1 resultantes de esta fase de destilación de ventaja están representadas en la figura 4. Y_1 se convierte entonces en la nueva referencia. Se constata que X_1 e Y_1 presentan una sola diferencia entre ellas (diferencia 12), frente cuatro diferencias entre X_0 e Y_0. Se comprende así que la destilación de ventaja puede hacer caer rápidamente el número de diferencias entre las cadenas numéricas del lector 1 y de la etiqueta 2.

Si el atacante 4 decide actuar como lo hacen el lector 1 y la etiqueta 2, aquél puede entonces captar los resultados de la O exclusiva intercambiados entre estos y deducir una cadena Z_1 según los mismos principios. Z_1 comprende entonces el primer bit de cada pareja de Z_0 que tenga el mismo rango que dos parejas correspondientes de X'_0 e Y_0 para los cuales ha sido obtenido el mismo resultado de la O exclusiva. Como se muestra en la figura 4, la cadena numérica Z_1 obtenida en el ejemplo comprende dos diferencias con Y_1 y siempre una diferencia con X_1.

La fase de destilación de ventaja puede ser repetida un número n de veces, siendo n entero, hasta que la cadena numérica X_n tenga una tasa de error con relación a Y_n inferior a un umbral elegido. Por ejemplo, el número n puede ser elegido en función del ruido estimado en el canal de comunicación 3.

En el ejemplo ilustrado en las figuras, es obtenida una identidad entre las cadenas numéricas del lector 1 y de la etiqueta 2 desde el segundo pase de la fase de destilación de ventaja. En efecto, como se muestra en la figura 5, las cadenas X_2 e Y_2 son idénticas.

Por el contrario, la cadena Z_2 obtenida, durante la segunda fase, por un atacante 4 que pone en práctica las mismas operaciones que el lector 1 y la etiqueta 2, permanece diferente de la cadena de referencia Y_2.

Se puede mostrar que cualquiera que sea el ruido presente en el canal ruidoso 3 y cualquiera que sea la técnica empleada por el atacante 4 para intentar descubrir las cadenas numéricas obtenidas por el lector 1 y/o la etiqueta 2, este atacante obtendrá siempre una cadena numérica errónea, es decir, diferente de la del lector 1 y de la etiqueta 2.

A continuación se pone en práctica una fase de reconciliación de información. Esta consiste en eliminar todavía errores residuales en la cadena numérica del lector 1 (o en la etiqueta 2 cuando la referencia es la cadena del lector), para los casos en que la destilación de ventaja no haya suprimido ya todos los errores.

En esta fase de reconciliación de información se utiliza un protocolo de corrección de error. Este protocolo deberá ser elegido de preferencia para hacer mínimas las informaciones que van a ser emitidas por el canal 3 y que podrían representar informaciones pertinentes explotables por el atacante 4.

Un ejemplo de protocolo es el protocolo “Cascade” descrito por G. Brassard y L. Salvail en el artículo “Secret-key reconciliation by public discussion, EURO-CRYPT ’93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology, Springer-Verlag New York, Inc. 1994, pp. 410-423”.

Con el protocolo Cascade, las dos partes de la comunicación se ponen de acuerdo aleatoria y públicamente sobre una permutación que ellas aplican respectivamente en las cadenas numéricas que han obtenido a la salida de la destilación de ventaja. El resultado de estas permutaciones es a continuación escindido en bloques de tamaño adaptable determinado. Para cada bloque así obtenido, se ejecuta una primitiva DICHOT. Cuando la paridad de los bloques correspondientes para las dos partes es idéntica, la primitiva calculada vuelve a la posición de una diferencia en el seno de estos bloques. Después una de las partes corrige este error. Están generalmente previstas etapas suplementarias llamadas de “bactracking” para asegurar que el conjunto que referencia todos los bloques cuya paridad ha sido modificada a continuación de la corrección de un error esté finalmente vacío.

De preferencia, se aplicará al lector 1 y a la etiqueta 2 un protocolo conocido inspirado en Cascade, pero en el cual (i) la permutación puesta en práctica es previamente cableada y no aleatoria, (ii) el tamaño de los bloques es fijo y no adaptable, y (iii) la bactracking no es puesta en práctica. La puesta en práctica de un tal protocolo aligerado tiene la ventaja de ser menos costoso que para Cascade, particularmente en términos de capacidad de cálculo y de tamaño de memoria. En la práctica, la mayoría de los errores son corregidos desde la primera fase, tan bien que los rendimientos de este protocolo aligerado son satisfactorios.

A la conclusión de la fase de reconciliación de información, el lector y la etiqueta 2 disponen de una misma cadena numérica con un nivel de probabilidad predeterminado. En el ejemplo descrito en referencia a las figuras, se anotan X_2^* e Y_2^* las cadenas numéricas idénticas así obtenidas por el lector 1 y la etiqueta 2, respectivamente, es decir, las cadenas X_2 e Y_2 después de la corrección. En cuanto al atacante, éste posee una cadena numérica Z_2^* que difiere de X_2^* e Y_2^*, gracias principalmente a la introducción inicial de los errores artificiales en X_0 e igualmente gracias a las propiedades de las fases de destilación de ventaja y de reconciliación de información.

Una tercera fase de dicha amplificación de secreto es puesta en práctica a continuación. El objeto de una tal fase ha sido divulgado por Charles H. Bennett, Gilles Brassard, Claude Crepeau y Ueli M. Maurer, en el artículo "Generalized privacy amplification, IEEE Transaction on information Theory (1995). Aquella consiste en aplicar una función de cálculo de clave a las cadenas numéricas obtenidas por el lector 1 y la etiqueta 2 a la conclusión de la fase precedente, es decir, a X_2^* e Y_2^* en nuestro ejemplo.

Una función de cálculo de clave es una función de compresión que permite obtener una información más corta de una información inicial a la cual se aplica. Aquella tiene además como propiedad suministrar resultados muy diferentes a partir de informaciones iniciales que difieren incluso ligeramente, es decir, que acentúan las diferencias entre informaciones distintas, de manera que se evita que se pueda volver a encontrar fácilmente la información inicial a partir del resultado del cálculo de clave.

Un ejemplo de la función de cálculo de clave que puede ser utilizado es el divulgado por Kaan Yüksel en el documento "Universal Hashing for ultra-low-power cryptographic hardware applications, Master's thesis, Worcester Polytechnic Institute, 2004". Esta función tiene la ventaja de requerir muy pocos recursos de cálculo, lo que está de acuerdo con las limitaciones de las etiquetas RFID.

El documento "Linking Information Reconciliation and Privacy Amplification, JOURNAL OF CRYPTOLOGY, 1997, páginas 1-12, CHRISTIAN CACHIN, UELI MAURER, USA", divulga un procedimiento de comunicación inalámbrica en un canal ruidoso, que comprende la transmisión de una primera cadena numérica, la recepción de una segunda cadena numérica correspondiente a la primera cadena numérica, a los errores introducidos por el canal ruidoso cercano, una fase de destilación de ventaja en la cual se determina una nueva cadena numérica a partir de la primera cadena numérica y se determina una nueva segunda cadena numérica a partir de la segunda cadena numérica, de manera que se toma ventaja sobre un eventual atacante pasivo; una fase de reconciliación de información en la cual se aplica un protocolo de corrección de errores a la nueva primera y a la nueva segunda cadenas numéricas, de manera que, a la salida de esta fase de reconciliación, la nueva primera y la nueva segunda cadenas numéricas sean idénticas con un nivel de probabilidad predeterminado; y una fase de amplificación de secreto en la cual se aplica una función de cálculo de clave a la nueva primera y a la nueva segunda cadenas numéricas.

La figura 6 muestra la aplicación de la función de cálculo de clave G a X_2^* e Y_2^*. Puesto que $X_2^* = Y_2^*$, se tiene también $G(X_2^*)=G(Y_2^*)$. De ese modo, el lector 1 y la etiqueta 2 disponen finalmente de una misma cadena numérica de tamaño limitado. En un caso real, $G(X_2^*)$ y $G(Y_2^*)$ son, por ejemplo, cadenas numéricas que comprenden del orden de una centena de bits.

A la inversa, el atacante 4 dispone de una cadena Z_2^* diferente de X_2^* e Y_2^*. Incluso si este atacante conoce la función de cálculo de clave utilizada por el lector 1 y la etiqueta 2, e intenta calcular $G(Z_2^*)$, obtendrá así una cadena numérica diferente de $G(X_2^*)$ y $G(Y_2^*)$.

En consecuencia, la cadena numérica $G(X_2^*)=G(Y_2^*)$ conocida para el lector 1 y la etiqueta 2 puede ser utilizada para asegurar los intercambios en el canal 3. Por ejemplo, esta cadena puede ser utilizada como una clave secreta que permite autenticar el lector 1 o la etiqueta 2, o bien cifrar los datos transmitidos por el canal 3 ruidoso, por ejemplo. Se pueden contemplar otras aplicaciones a partir de la determinación de esta clave secreta.

REIVINDICACIONES

1. Procedimiento de comunicación entre un lector de identificación sin hilo (1) y un marcador de identificación sin hilo (2) por intermedio de un canal ruidoso (3), que comprende:

/a/ la transmisión de una primera cadena numérica (X_0) desde el lector hacia el marcador;
/b/ la recepción, en el marcador, de una segunda cadena numérica (Y_0) correspondiente, en la primera cadena numérica, a los errores introducidos por el canal ruidoso;
/c/ la introducción de errores artificiales al menos en una de la primera y de la segunda cadenas numéricas;
/d/ una fase de destilación de ventaja en la cual se determina, en el lector, una nueva primera cadena numérica (X_1) a partir de la primera cadena numérica y se determina, en el marcador, una nueva segunda cadena numérica (Y_1) a partir de la segunda cadena numérica, de manera que se toma ventaja sobre un eventual atacante pasivo;
/e/ una fase de reconciliación de información en la cual se aplica un protocolo de corrección de errores a la nueva primera (X_2) y a la nueva segunda (Y_2) cadenas numéricas, de manera que, a la salida de la etapa /e/, la nueva primera (X_2*) y la nueva segunda (Y_2*) cadenas numéricas son idénticas con un nivel de probabilidad predeterminado; y
/f/ una fase de amplificación de secreto en la cual se aplica una función de cálculo de clave (G) a la nueva primera (X_2*) y a la nueva segunda (Y_2*) cadenas numéricas.

2. Procedimiento según la reivindicación 1, en el cual la fase de destilación de ventaja comprende las etapas siguientes:

- se descomponen en grupos de N valores numéricos sucesivos, siendo N entero, la primera (X'_0) y la segunda (Y_0) cadenas numéricas;
- se efectúa una O exclusiva sobre cada uno de los citados grupos;
- se intercambian los resultados de la O exclusiva entre el lector y el marcador;
- se determina, en el lector, la nueva primera cadena numérica (X_1) a partir del primer valor numérico de cada grupo de la primera cadena numérica para el cual el resultado de la O exclusiva es idéntico al resultado de la O exclusiva efectuada sobre el grupo correspondiente de la segunda cadena numérica; y
- se determina, en el marcador, la nueva segunda cadena numérica (Y_1) a partir del primer valor numérico de cada grupo de la segunda cadena numérica para el cual el resultado de la O exclusiva es idéntico al resultado de la O exclusiva efectuada sobre el grupo correspondiente de la primera cadena numérica.

3. Procedimiento según la reivindicación 1 o la 2, en el cual la introducción de errores artificiales de la etapa /c/ comprende una modificación aleatoria de valores numéricos de una al menos de la primera (X_0) y de la segunda (Y_0) cadenas numéricas.

4. Procedimiento según una cualquiera de las reivindicaciones precedentes, en el que la etapa /d/ es repetida un número de veces con dependencia del ruido estimado sobre el canal ruidoso (3).

5. Procedimiento según una cualquiera de las reivindicaciones precedentes, en el cual el protocolo de corrección de errores es elegido de manea que se deje escapar un mínimo de información hacia un eventual atacante pasivo.

6. Lector de información sin hilo (1) apto par comunicar con un marcador de identificación sin hilo (2) por intermedio de un canal ruidoso (3), que comprende:

- medios para transmitir una primera cadena numérica (X_0) hacia el marcador;
- medios para introducir errores artificiales en la primera cadena numérica;
- medios para determinar una nueva primera cadena numérica (X_1) a partir de la primera cadena numérica, de manera que se tome ventaja sobre un eventual atacante pasivo;
- medios para aplicar un protocolo de corrección de errores a la nueva primera cadena numérica (X_2); y
- medios para aplicar una función de cálculo de clave (G) a la nueva primera cadena numérica (X_2*).

7. Marcador de identificación sin hilo (2) apto para comunicar con un lector de identificación sin hilo (1) por intermedio de un canal ruidoso (3), que comprende:

- medios para recibir una segunda cadena numérica (Y_0) correspondiente, en la primera cadena numérica (X_0) transmitida por el lector, a los errores introducidos por el canal ruidoso cercano;
- medios para introducir errores artificiales en la segunda cadena numérica;
- medios para determinar una nueva segunda cadena numérica (Y_1) a partir de la segunda cadena numérica, de manera que se tome ventaja sobre un eventual atacante pasivo;

- medios para aplicar un protocolo de corrección de errores a la nueva segunda cadena numérica (Y_2); y
- medios para aplicar una función de cálculo de clave a la nueva segunda cadena numérica (Y_2*).

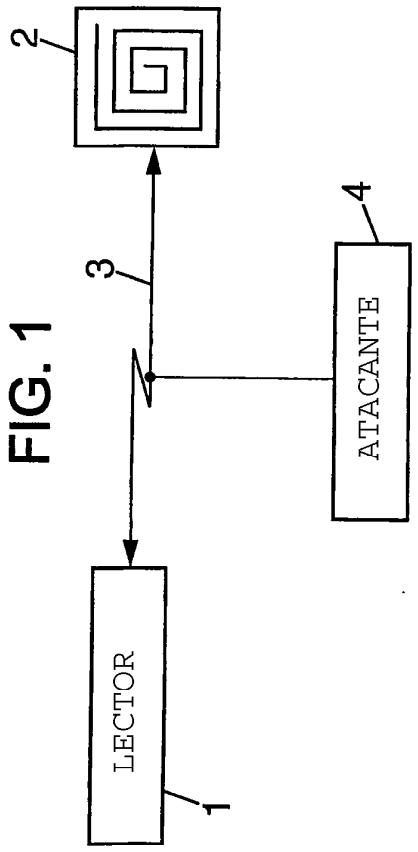

FIG. 1

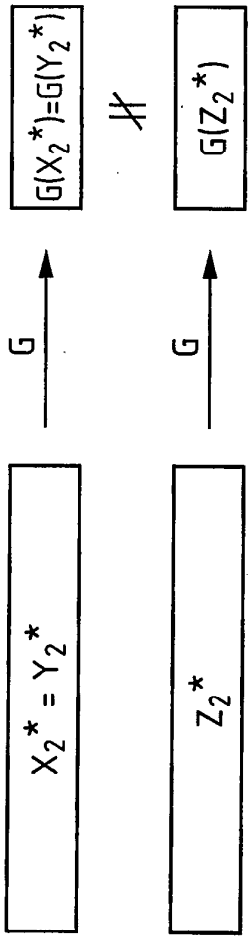

FIG. 6

FIG. 5

$X_2 = [\ 0\ 1\ 1\ ]$

$Y_2 = [\ 0\ 1\ 1\ ]$

$Z_2 = [\ 0\ 0\ 1\ ]$

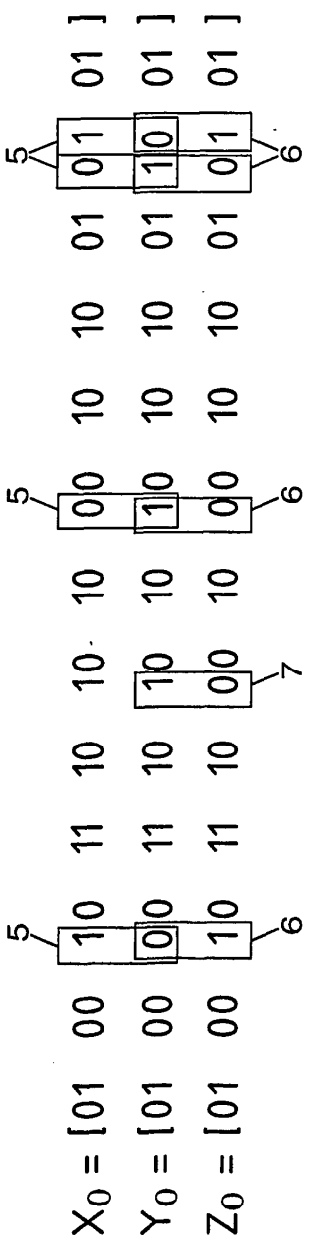

FIG. 2

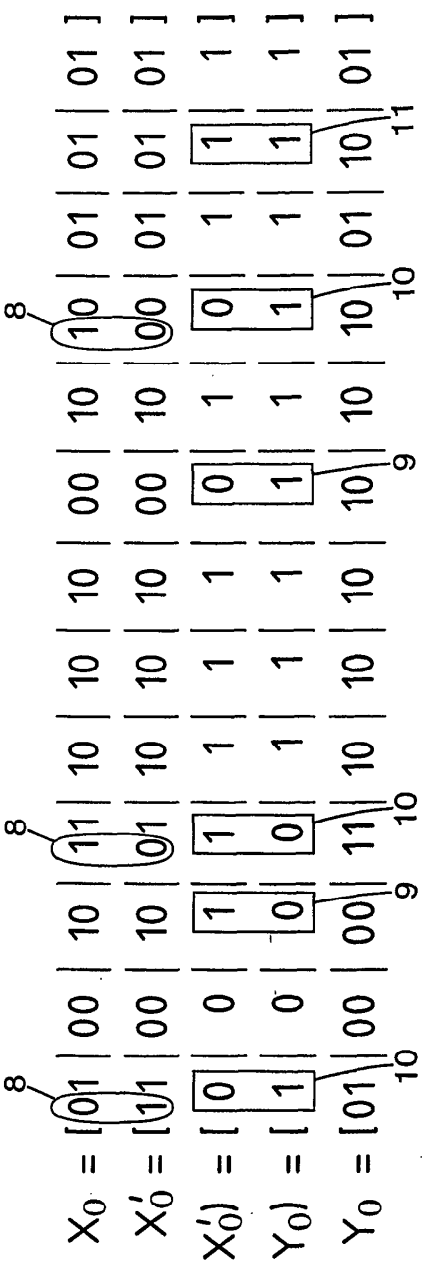

FIG. 3

FIG. 4