Una propuesta para el uso de códigos QR en la autenticación de usuarios

Luis Hernández Encinas
Instituto de Seguridad de la Información (ISI)
Consejo Superior de Investigaciones Científicas (CSIC)
Email: luis@iec.csic.es

Alberto Peinado Domínguez
Dept. Ingeniería de Comunicaciones
E.T.S.I. Telecomunicación, Universidad de Málaga
Email: apeinado@ic.uma.es

***Resumen*—En este trabajo se presentan las posibilidades que ofrecen los códigos bidimensionales QR en la implementación de esquemas y protocolos criptográficos. Así, se analiza la utilización actual de estos códigos determinando los principales problemas de seguridad que podrían surgir y se repasan algunas de las aplicaciones más significativas de códigos QR relacionadas con determinados usos criptográficos. Finalmente, se presenta una propuesta de autenticación para el control de acceso a recintos, que aúna las dos grandes ventajas que ofrecen estos códigos: un canal de comunicación seguro y la facilidad que ofrecen para el intercambio de datos entre dispositivos.**

I. Introducción

Los códigos QR son códigos bidimensionales formados por una matriz de propósito general diseñada para un escaneo rápido de información. Su nombre procede de "Quick Response" (respuesta rápida) ya que se diseñó para ser decodificado a alta velocidad ([13]). El código QR es un código abierto, de ahí su extensa utilización. Presentan una forma cuadrada y están caracterizados por tres cuadros más pequeños, ubicados en la parte superior e inferior izquierda, que permiten identificar la posición del código al lector (ver Figura 1).

Figura 1. Ejemplo de código QR

Las principales características de estos códigos son:

- *Alta velocidad de decodificación*: Están diseñados para minimizar el tiempo de decodificación. Esto permite utilizarlos en una gran variedad de aplicaciones así como en dispositivos con recursos de computación limitados.
- *Bajo coste del decodificador*: A diferencia de los códigos de barras unidimensionales, que necesitan lectores láser para la lectura y decodificación, los códigos bidimensionales QR sólo necesitan una cámara de baja resolución para capturar la imagen del código y un software para procesarla. Esto permite utilizar la cámara de un teléfono móvil o una webcam. En cuanto al software del decodificador, existen numerosas implementaciones de uso libre o código abierto y librerías para programar aplicaciones específicas en distintos lenguajes.
- *Facilidad de lectura*: Su diseño posibilita que sean leídos en cualquier posición. Las marcas que aparecen en tres de sus esquinas permite reorientarlo automáticamente una vez que ha sido capturado por la cámara.
- *Gran capacidad de codificación de datos*: La capacidad de los datos que puede almacenar un código QR depende del tipo de dato, pero en cualquier caso, es superior a la de otros códigos bidimensionales. Así, si los datos son numéricos, se puede llegar hasta un máximo de 7.089 caracteres; si los datos son alfanuméricos, el máximo es de 4.296 caracteres; mientras que si los datos son binarios, el número máximo es de 2.953 bytes.
- *Codificación extendida*: Posibilidad de codificar más tipos de datos que otros de códigos bidimensionales, entre ellos los caracteres Kanji y Kana.
- *Gran resistencia frente a errores*: Se pueden restaurar los datos contenidos en un código QR aunque parte del mismo esté dañada o manchada. De hecho, es posible restaurar hasta el 7 % para los códigos de nivel L, un 15 % para el nivel M, un 25 % para el nivel Q y un 30 % para el máximo nivel de corrección, el H.
- *Posibilidad de personalización*: Debido a la alta resistencia frente a errores, estos códigos pueden ser personalizados añadiéndoles color, superponiendo algún elemento propio de la imagen corporativa de quien emite el código o modificando ligeramente alguna parte del código.
- *Adaptación al tamaño de los datos*: En función de la cantidad de datos a codificar, el estándar permite utilizar hasta 40 versiones del código QR. Cada versión tiene mayor capacidad de codificación que la anterior, de tal modo que la versión se puede asimilar al tamaño de los datos que almacena el código generado. Cuantos más datos se desee codificar mayor será la versión. Sin embargo, la versión no implica necesariamente un mayor tamaño de impresión o visualización. Las versiones quedan definidas por el número de módulos que se utilizan para su representación. En función de la

resolución de la impresión, los códigos tendrán un mayor o menor tamaño. Así se pueden encontrar códigos QR con tamaños para insertar en una tarjeta de visita o en una valla publicitaria.

Aunque los códigos QR se crearon con fines de inventario y logística, sus características, junto con la gran popularidad de los móviles con cámara y tablets y la conectividad a Internet, ha dado lugar a usos alternativos de estos códigos, dando nacimiento al concepto de "hardlinking" o "enlace físico".

Hoy en día es fácil ver estos códigos por todos lados. Su utilización ha traspasado fronteras y desde hace unos años se pueden encontrar en una gran diversidad de lugares y aplicaciones: restaurantes, turismo, servicios gubernamentales, etc. Sin duda alguna, las campañas publicitarias han ayudado en gran medida a su difusión.

El principal uso de los códigos QR consiste en capturarlos con la cámara de un dispositivo móvil (teléfono, tablet, etc.) y decodificar la información que contiene. Esta información suele ser una URL que conduce al usuario a un sitio web en el que se ofrece información adicional relacionada con el producto al que está asociado el código QR. En otras ocasiones se utiliza simplemente como enlace a los perfiles de redes sociales, o como medio de transporte de información, como por ejemplo las tarjetas de visita en formato VCARD ([17]).

De una u otra manera, los códigos QR se han convertido ya en un canal de comunicación que permite llegar a un gran número de usuarios de un modo sencillo y a bajo coste. Por este motivo, se hace necesario realizar un análisis sobre la seguridad de las comunicaciones y transacciones que se realizan mediante códigos QR, así como estudiar sus posibles aplicaciones a la criptografía.

El resto del contenido de este trabajo se distribuye de la siguiente manera. En la sección II se describen los códigos QR, incluyendo sus usos más extendidos y sus principales debilidades en materia de seguridad. Algunas cuestiones relacionadas con el uso de los códigos QR y la criptografía se comentan en la sección III. En la sección IV se propone la utilización de los códigos QR para la autenticación de individuos mediante su identidad y por medio de tokens. La sección V recoge tanto el análisis de la propuesta como algunos resultados experimentales relacionados con la misma. Finalmente, la sección VI contiene las conclusiones.

II. Los códigos QR

II-A. Principales usos de los códigos QR

Los códigos QR fueron desarrollados por la empresa japonesa Denso-Wave en 1994 para controlar la producción de piezas de automóviles Toyota. Cada pieza llevaba un código que la identificaba. A través de cámaras se capturaba y decodificaba cada código, con lo que cada pieza que pasaba por determinados puntos de control quedaba identificada. El estándar japonés fue publicado en enero de 1999 y su correspondiente estándar internacional ISO fue aprobado en junio de 2000 ([7], [8]).

Actualmente, las aplicaciones de los códigos QR se pueden clasificar en dos grandes grupos: los que utilizan códigos QR impresos en alguna superficie (según el esquema original) y los que utilizan una pantalla para mostrar el código, sin necesidad de utilizar ningún soporte para imprimirlo.

En el primer grupo se encuentran las aplicaciones publicitarias en las que el código aparece insertado en algún cartel, fotografía, folleto, etc., de forma que los usuarios puedan fotografiarlo o leerlo directamente con su dispositivo móvil y enlazar con un sitio web en el que se le mostrará más información.

Otras aplicaciones de este mismo grupo facilitan a los usuarios la transferencia de determinado tipo de información, como la de una tarjeta de visita o una clave criptográfica pública. Son muchos los profesionales que codifican sus datos personales utilizando el formato VCARD dentro de un código QR. De este modo, en lugar de teclear los datos en la agenda del dispositivo, se lee el código QR de la tarjeta y automáticamente se incorporan los datos a la agenda. Las redes sociales también emplean estos códigos para proporcionar enlaces a los perfiles de usuarios. En lugar de introducir la URL completa, que a veces puede ser complicada de transcribir, se lee el QR y automáticamente el dispositivo se conecta al perfil deseado.

En el segundo grupo de aplicaciones se encuentran aquellas que muestran el código QR en una pantalla, lo que proporciona mayor dinamismo al esquema, puesto que el símbolo puede ser modificado por el sistema de soporte, y por tanto, la duración del símbolo es mucho más corta. Algunos ejemplos son las aplicaciones que emiten billetes electrónicos basados en QR de modo que para acceder a un avión solo es necesario mostrar el código en la pantalla del dispositivo y acercarlo a un dispositivo lector o cámara para que sea reconocido ([3]). En otros casos se utilizan en páginas web para transmitir al usuario unas credenciales que le permitan acceder al sistema en otro momento. La compañía Sony, por ejemplo, utiliza los códigos QR en la nueva Nintendo 3DS para traspasar los perfiles Mii creados por un usuario a otro.

En todo caso, los códigos QR proporcionan una manera de comunicar información a través de los datos (texto) que codifican o de la URL a la que direccionan. Se pueden considerar como parte integrante del nuevo paradigma conocido como la Internet de las cosas.

II-B. Riesgos de los códigos QR

La utilización de los códigos QR está llena de potenciales peligros debido a una combinación de factores, entre los que se encuentran la facilidad de uso por parte de los usuarios, la integración de los decodificadores en los dispositivo móviles y la gran difusión y aceptación que están teniendo gracias a las campañas publicitarias que suelen incorporar descuentos y promociones.

La raíz del problema reside en el hecho de que los códigos QR son símbolos gráficos que una vez impresos en algún soporte quedan expuestos permanentemente al público. En principio, esto no supone ningún problema ya que la información que contienen es de carácter público y el principal objetivo es la difusión de la misma, por ejemplo, la URL del sitio web de una marca publicitaria.

Precisamente porque la difusión es el fin primordial en la mayoría de los casos, el contenido de los códigos QR es texto en claro. Esto convierte a los códigos QR en una herramienta muy valiosa para los ciberataques, puesto que cualquier atacante puede generar un código QR que contenga una URL parecida, pero con contenido malicioso, y sustituirla por la original. El método es sencillo: se imprime el código QR malicioso en una pegatina que se coloca encima del código QR original; o se puede generar directamente una campaña falsa creando folletos con la imagen de una marca conocida que sirva de reclamo. El resultado en cualquier caso es que los usuarios al decodificar el símbolo QR serán dirigidos a una URL que tiene unos fines completamente diferentes a los que el usuario podría imaginar.

Algunas de las posibles consecuencias son las siguientes:

- En el caso más sencillo, los usuarios pueden ser simplemente engañados para que visiten una web aprovechando el reclamo de una marca que nada tiene que ver con la información que realmente se muestra. Esta situación, aunque no compromete la seguridad del sistema, puede causar graves daños de imagen a la marca que se utiliza como reclamo.
- En otras ocasiones, las URL a las que conducen los códigos QR contienen formularios que solicitan información de carácter personal al usuario. Este tipo de técnicas para recopilar datos de futuros objetivos publicitarios es muy frecuente. Es el usuario el que decide si ceder sus datos para que le envíen más publicidad. Sin embargo, si la URL no es auténtica, estos datos de carácter personal podrían ser utilizados con otros fines. En general, no es aconsejable responder a este tipo de formularios, puesto que, como es sabido, el phishing es mucho más efectivo que otras técnicas de criptoanálisis para conseguir las credenciales (claves y contraseñas) de los usuarios.
- Por último, las URL falsas pueden contener código malicioso que se instala en los dispositivos de los usuarios cuando acceden al sitio web. Estos códigos maliciosos pueden acceder a los datos privados que están almacenados en el dispositivo. Ello es posible gracias a que la gran mayoría de los dispositivos móviles no incorporan un software de seguridad para impedir estos ataques.

II-C. Recomendaciones de seguridad de los códigos QR

Aunque los usuarios son cada vez más conscientes de la importancia de la seguridad de sus ordenadores personales, no se presta la misma atención a la seguridad de los dispositivos móviles (teléfonos, tablets, etc.). La situación comienza a ser preocupante debido a la gran cantidad de usuarios que se conectan habitualmente a Internet desde estos dispositivos.

A continuación se presentan algunas recomendaciones para minimizar, y en lo posible evitar, los ciberataques que aprovechan los códigos QR.

- *Comprobación del decodificador*. Debido a que es un estándar abierto, existe una gran cantidad de aplicaciones de libre distribución que una vez instalada en el dispositivo decodifica el código QR ([1], [5]). Es importante verificar que estas aplicaciones solo decodifican y no hacen ninguna otra cosa que podría comprometer al sistema.
- *Elección del decodificador*. Aunque el decodificador funcione correctamente, el software que se ejecuta en el dispositivo puede funcionar de muchas formas. Hay algunas aplicaciones que intentan conectar directamente con la URL decodificada. Es recomendable que el software utilizado solo muestre en pantalla el resultado de la decodificación para que el usuario indique posteriormente si desea conectarse o no a la URL.
- *Formularios*. Como norma general, no es recomendable responder a formularios ni facilitar datos de carácter personal.
- *Software de seguridad*. Es recomendable que todos los dispositivos que realicen conexiones a Internet dispongan de un software de seguridad que los proteja de los códigos maliciosos que pueden colarse a través de URL fraudulentas.

Como ya se ha mencionado anteriormente, los problemas de seguridad se derivan de la falta de autenticación. Si los usuarios pudieran verificar que los símbolos QR decodificados son auténticos, es decir, que no han sido generados por terceras partes que están suplantando al emisor real, entonces, se podrían detectar todos estos ataques.

III. Criptografía y códigos QR

III-A. Usos criptográficos de los códigos QR

A pesar de los problemas de seguridad que plantea la utilización de los códigos QR, el canal de comunicación se puede considerar seguro, desde un punto de vista criptográfico, si la captura del símbolo QR se realiza sin soporte físico, es decir, si se captura la foto mostrada en una pantalla, puesto que la posibilidad de interceptar la comunicación es muy baja. En consecuencia, las técnicas criptográficas deberían estar encaminadas a proteger otros aspectos del sistema. A continuación se describen las aplicaciones criptográficas más significativas de los códigos QR.

Dado que el uso principal de los códigos QR es el de transmitir información pública, el principal servicio criptográfico es la autenticación. No es importante ocultar la información que contiene el código, pero sí es necesario autenticarla. Un usuario que decodifique un código debería poder comprobar si es auténtico o si ha sido modificado con un objetivo malicioso. Sin embargo, la mayoría de los sistemas propuestos hasta ahora han desarrollado aplicaciones con otros objetivos.

Uno de ellos consiste en utilizar códigos QR cifrados. En este caso, estos códigos pierden gran parte de su funcionalidad puesto que aunque puedan ser decodificados por el público general, no todo el mundo puede acceder a la información original, es decir, descifrarlos. La prioridad aquí es aprovechar la facilidad de transmisión de información, pero no la capacidad de difusión de la misma. Este sistema, propuesto y desarrollado por Quickmark ([14]), es posible gracias a que el estándar QR es abierto y se puede incluir el cifrado y descifrado en el codificador y decodificador.

Siguiendo la misma filosofía, en [18] se propone la utilización del criptosistema RSA ([15]) para cifrar la información contenida en el código QR.

Los tickets electrónicos basados en códigos QR son otro ejemplo de este uso criptográfico. En [3] se define un sistema que tras comprar el ticket a través de Internet utilizando un teléfono móvil, el vendedor envía una identificación única al comprador. Éste lo cifra con un sistema simétrico (AES, [12]) utilizando como clave una contraseña elegida por el comprador. El resultado se codifica como un código QR que es lo que el comprador presentará cuando acceda físicamente al establecimiento. Como el contenido del código QR está cifrado, el comprador debe introducir de nuevo su contraseña en el dispositivo lector del establecimiento para que éste pueda descifrarlo. Para comprobar que el ticket es válido el sistema almacena el resumen (hash) del identificador cifrado.

Existen otras muchas aplicaciones desarrolladas para Android que facilitan el uso de códigos QR con determinados tipos de sistemas de cifrado (ver [1], [5]).

Todos estos sistemas se centran en cifrar el código para proteger la posible pérdida o robo del mismo, o del dispositivo en el que se almacena, y evitar la realización de copias no autorizadas o la generación de códigos no válidos.

III-B. Autenticación con códigos QR

Una aproximación para la autenticación de usuarios mediante códigos QR podría ser la utilización de criptosistemas de clave pública, que permiten de un modo natural la implementación de esquemas de firma digital ([18]). Sin embargo, la longitud de las firmas son, en general, demasiado grandes como para permitir un uso eficiente de estos métodos. Recuérdese que el criptosistema RSA genera firmas de longitud grandes (entre 1.024 y 2.048 bits), mientras que la capacidad de los códigos QR en sus versiones más manejables (de la 2 a la 13) tienen una capacidad total de 256 (v2) a 3.400 bits (v13), cuando se aplica el menor nivel de corrección de errores (nivel L) y de 112 (v2) a 1.416 bits (v13) cuando se aplica el máximo (nivel H).

Aunque los criptosistemas de clave pública basados en curvas elípticas, ECC ([6]), utilizan claves mucho menores con la misma seguridad (1.024 bits RSA equivalen a 160 bits ECC, [11]), estos sistemas necesitan una infraestructura de clave pública para que funcionen correctamente. Todo ello complica la utilización de los códigos QR puesto que sería necesario distribuir a todos los usuarios las claves públicas de todos aquellos que quisieran generar códigos QR autenticados.

Por otra parte, son conocidos los criptosistemas basados en la identidad del usuario ([16]), que pueden ser utilizados para definir un esquema de firma. Estos sistemas se diseñaron para reducir, entre otras cosas, la complejidad global utilizando la propia identidad del usuario (como su dirección de correo electrónico, por ejemplo) en lugar de hacer uso de certificados digitales ([2]). En [9] se propone una implementación de cifrado y firma basado en la identidad con sistemas RFID (Radio Frequency IDentification, [4]). En [10] se propone un sistema basado en la identidad para autenticar etiquetas de RFID pasivas empleadas en señales de tráfico.

Es de destacar un paralelismo entre las etiquetas RFID de [10] y los códigos QR en el sentido de que ambos métodos son elementos pasivos que contienen determinada información, de modo que sólo es obligatoria la autenticación. La confidencialidad no es imprescindible; las etiquetas RFID y los códigos QR pueden estar expuestos públicamente por un periodo de tiempo ilimitado.

En general, la implementación de este tipo de esquemas precisa de la existencia de un tercero de confianza o centro de generación de claves (Key Generation Center, KGC). El KGC genera, en primer lugar, su clave maestra, que mantiene en secreto y una clave pública asociada. A continuación genera (o ayuda a generar) la clave privada de cada usuario, la cual está asociada a la identidad de dicho usuario.

En el caso de los sistemas basados en RFID, la clave puede ser cargada en cada etiqueta y en el lector antes del despliegue del sistema. La ventaja más importante de estos esquemas recae en el mecanismo de obtención de la clave pública de otro usuario.

En los criptosistemas basados en la identidad, cada usuario puede generar la clave pública de otro usuario utilizando la información del firmante y la clave pública del KGC. De este modo no es preciso establecer conexión alguna para verificar las firmas contenidas en el código QR. Así, los esquemas de firma basados en la identidad parecen ser los más adecuados para los códigos QR, aunque es preciso llevar a cabo más investigaciones dado que la criptografía basada en la identidad se fundamenta en la criptografía asimétrica y la complejidad computacional que ésta lleva aparejada debe ser tenida en consideración cuando se emplean dispositivos con poca capacidad computacional.

IV. Propuesta de un esquema de autenticación basado en códigos QR

El esquema que se propone a continuación tiene como objetivo autenticar usuarios mediante el uso de códigos QR y de dispositivos móviles. La aplicación más inmediata es el control de acceso físico a recintos protegidos mediante la autenticación de usuarios basada en tokens. En este caso, se trata de emplear dos de los requisitos que habitualmente se utilizan para la autenticación: algo que se posee (un dispositivo móvil, que se denominará *token* en lo que sigue) y algo que se conoce (una clave).

IV-A. Fase de registro

Como otros muchos sistemas de autenticación, en este caso se requiere una fase de registro en la que el usuario U_i proporciona su identificación, ID_i, al KGC quien, previa comprobación de la identidad real del usuario, determina una clave secreta de determinado sistema de cifrado simétrico, por ejemplo, AES, K_i, que será insertada en el *token* del usuario y que compartirá con el servidor del sistema, S.

1. El usuario U_i solicita ser incluido en la base de datos de aquellos que tienen acceso a determinado servicio,

enviando su identificación, ID_i, al KGC:

$$U_i \rightarrow solicitud(ID_i) \rightarrow KGC.$$

2. KGC comprueba que la identificación recibida corresponde, efectivamente, a la identidad del usuario U_i.
3. KGC genera una clave secreta, K_i, para U_i, que es insertada en la aplicación correspondiente de su *token* y protegida por un password, k_i, que es suministrado a dicho usuario.
   Eventualmente, KGC puede utilizar, además de la identificación del usuario, una identificación del *token*, T_i, como por ejemplo el IMEI del móvil, para generar la clave K_i.

$$U_i \leftarrow k_i \leftarrow token \leftarrow \{ID_i, [T_i], K_i\} \leftarrow KGC.$$

4. KGC envía, por un canal seguro y autenticado, el conjunto de valores $\{ID_i, [T_i], K_i\}$ a S.

Nótese que no es necesario que S sea la misma entidad que KGC. De hecho, si ambas son diferentes, el sistema sólo será capaz de asociar a cada identificación, ID_i, su clave secreta correspondiente, K_i, (y, eventualmente, el identificador del *token*, T_i) sin conocer más datos de U_i.

IV-B. Fase de acceso

El sistema que controla el acceso al recinto protegido, S, dispondrá de un dispositivo con una pequeña pantalla colocada junto a la puerta del recinto cuyo acceso se va a controlar. El protocolo para la autenticación del usuario es un protocolo de tipo desafío-respuesta, consistente en los siguientes pasos:

1. S genera un mensaje aleatorio, m, determina su código QR y lo muestra en su pantalla. Este código QR hace el papel de desafío y se denota por $D = QR(m)$.
   El procedimiento puede establecerse de modo que la pantalla del dispositivo muestre un código QR cuando el usuario pulse una tecla, se solicite el acceso, cuando haya transcurrido determinado periodo de tiempo, etc.
2. El usuario, U_i, acerca su *token* a la pantalla y escanea o captura el desafío mostrado, $D = QR(m)$, haciendo uso de la cámara de su *token* y de la aplicación correspondiente.
3. El usuario decodifica el desafío, D, obteniendo el mensaje aleatorio generado por S:

$$QR^{-1}(D) = QR^{-1}(QR(m)) = m.$$

4. U_i cifra dicho mensaje mediante la aplicación residente en el *token* y su clave secreta, K_i, obteniendo $M = AES_{K_i}(m)$, para lo cual hace falta que el usuario introduzca su password, k_i.
5. La respuesta al desafío, R, se forma mediante la unión de la identificación de U_i, ID_i, y el mensaje cifrado, M: $R = ID_i||M$ (y, eventualmente, con la identificación del *token*, T_i: $R = ID_i||T_i||M$).
   Dicha respuesta se codifica como un código QR, $QR(R)$, se muestra en la pantalla del *token* y se presenta para ser leída por el dispositivo del sistema, S.
6. S lee el código mostrado, $QR(R)$, y lo decodifica obteniendo la respuesta al desafío

$$QR^{-1}(QR(R)) = R = ID_i||M$$

   (eventualmente, $R = ID_i||T_i||M$). A partir de este valor, S obtiene la identificación del usuario, ID_i, (la del *token*, T_i) y el mensaje, M, cifrado con la clave K_i.
7. S calcula $AES^{-1}_{K_i}(M) = \bar{m}$ y comprueba si se verifica la igualdad $\bar{m} = m$. En caso afirmativo, U_i ha sido autenticado (y, eventualmente, también su *token*) de modo que S abre la puerta para permitirle el acceso.

La presentación de la respuesta $R = ID_i||M$ por el usuario a S puede hacerse de modo que el código QR presentado en la pantalla del *token*, $QR(R)$, contenga el identificador del usuario, ID_i, sobreimpreso a dicho código (véase el código izquierdo de la Figura 2), o de modo que $QR(R)$ sea un código QR normal, que contenga como parte de su información codificada a ID_i (véase el código derecho de la Figura 2).

Figura 2. Respuesta con código QR e Identificación

En el primer caso, el dispositivo del sistema debe utilizar un procedimiento para el reconocimiento de caracteres, de modo que pueda extraer el ID_i que está sobreimpreso al propio código. Desde un punto de vista conceptual, este método supone la utilización de diferentes canales de comunicación para el envío de la respuesta y de ID_i. Una ventaja de este método es que el valor de ID_i no ocupa espacio en el QR.

En el segundo caso, el código QR se muestra como un QR normal, pero de modo que el código incluya tanto M como ID_i. En este caso, no es preciso el uso del reconocimiento de caracteres. Sin embargo, tiene el inconveniente de que el código, al incluir el ID_i, permite menor espacio para el mensaje de desafío, m, generado por el sistema.

V. Análisis y resultados experimentales

La principales características de la propuesta presentada son las siguientes:

- Se basa en un protocolo de desafio/respuesta, lo que tradicionalmente es considerado como un método eficiente y eficaz de autenticación.
- No es preciso llevar a cabo una sincronización con el servidor como ocurre en sistemas de autenticación basados en contraseñas de un solo uso (tipo OTP), porque el *token* responderá cuando captura el desafío.

- No es necesario establecer sellos temporales porque el propio sistema presenta desafíos cada cierto tiempo.
- No es posible recuperar las respuestas que dan distintos usuarios ante el mismo desafío, D, ya que el canal de comunicación establecido a través del QR es seguro. En efecto, basta tener en cuenta que la respuesta, R, se muestra en la pantalla del *token* y su código QR correspondiente se presenta a la cámara del sistema.
- Es segura contra ataques por fuerza bruta, dado que un ataque de este tipo debería llevarse a cabo on-line, es decir, se debería responder adecuadamente al QR mostrado en la pantalla del sistema. Téngase en cuenta que la respuesta hace uso de la clave secreta, K_i, del usuario (y, eventualmente, de la identificación del *token*), que sólo es accesible por dicho usuario.

Se han llevado a cabo algunas pruebas para tratar de determinar la zona que resulte más eficiente para sobreimprimir el identificador del usuario, caso de que se opte por esta posibilidad. El objetivo de emplear esta opción es el de utilizar dos canales de comunicación independientes: el contenido del QR y la imagen del QR.

Analizando los resultados del Cuadro I, se observa que en el caso de utilizar una etiqueta horizontal, el área que se puede utilizar para superponer la etiqueta es menor que si se utiliza una etiqueta vertical. Como consecuencia de esto, se deduce que el porcentaje de corrección del código empleando etiquetas verticales está próximo al $30\,\%$, por tanto cerca del máximo que es posible alcanzar con el nivel H.

Cuadro I
COMPARACIÓN DE CÓDIGOS QR DE NIVEL H, VERSIONES 7–13, CON ETIQUETA HORIZONTAL Y VERTICAL SUPERPUESTA

Version	Porcentaje de corrección horizontal	Porcentaje de corrección vertical
7	$11{,}95\,\%$	$23,65\,\%$
8	$5{,}68\,\%$	$23,31\,\%$
9	$6{,}89\,\%$	$26,46\,\%$
10	$7{,}75\,\%$	$25,97\,\%$
11	$7{,}65\,\%$	$26,72\,\%$
12	$6{,}79\,\%$	$26,83\,\%$
13	$6{,}4\,\%$	$23,63\,\%$

VI. CONCLUSIÓN

Las propiedades de los códigos bidimensionales QR permiten su aplicación en los esquemas de autenticación y control de acceso proporcionando un canal de comunicación rápido y seguro entre las partes intervinientes, minimizando la posibilidad de que un atacante tenga acceso a los datos intercambiados. Este hecho, junto a la capacidad de almacenamiento de datos de estos códigos y a la versatilidad de los terminales telefónicos y tablets actuales, permite implementar mecanismos de autenticación basados en *token*.

En este trabajo, además de analizar la utilización criptográfica de estos códigos de un modo general, se ha presentado una propuesta concreta que hace uso tanto del canal seguro que proporciona el QR como de la facilidad que ofrece para el intercambio de datos. La propuesta se basa en un esquema desafío/respuesta donde un dispositivo ofrece el desafío en forma de código QR que es capturado por el usuario para calcular la respuesta mediante un algoritmo criptográfico de clave simétrica y devolverla también en forma de código QR.

Si se consideran, por ejemplo, desafíos y respuestas de 128 bits, identificadores de usuarios de 64 bits y 15 dígitos numéricos para la identificación del *token*, se necesitarían códigos QR que permitan la codificación de unos 240 bits aproximadamente, puesto que un QR puede codificar tres dígitos numéricos en un solo byte. Por tanto, se podrían utilizar códigos QR desde de la versión 4.

Sin embargo, la opción de superponer la identificación del usuario directamente sobre el código QR requiere utilizar versiones algo mayores con objeto de que la modificación o error que provoca esta superposición no afecte a la decodificación. Se recomienda utilizar versiones mayores o iguales de 7 con etiquetas verticales.

AGRADECIMIENTOS

Trabajo parcialmente subvencionado por el Ministerio de Ciencia e Innovación con los proyectos TIN2011-22668 y TIN2011-25452.

REFERENCIAS

[1] Andoid Market, http://www.androidmarket.es/e
[2] J. Baek, J. Newmarch, R. Safavi-Naini, and W. Susilo, “A survey of identity-based cryptography”, Proc. of the 10th Annual Conference for Australian Unix User’s Group, pp. 95–102, 2004.
[3] D. Conde, E. Costa, F.J. González, and F. Gil, “Secure eTickets based on QR-Codes with user-encrypted content”, International Conference on Consumer Electronics (ICCE), pp. 257–258, 2010.
[4] K. Finkenzeller, RFID Handbook, 2nd edition, Wiley, 2002.
[5] Google Play, https://play.google.com/store
[6] D. Hankerson, A.J. Menezes, and S. Vanstone, “Guide to Elliptic Curve Cryptography”, Springer-Verlag, New York, NY, USA, 2004.
[7] International Organization for Standardization/International Electrotechnical Commission, “Information technology–automatic identification and data capture techniques–bar code symbology–QR code”, ISO/IEC 18004, 114 pp., 2000.
[8] International Organization for Standardization/International Electrotechnical Commission, “Information technology. Automatic identification and data capture techniques. QR Code 2005 bar code symbology specification”, ISO/IEC 18004:2006, 126 pp., 2007.
[9] Y. Lian, and C. Rong, “RFID system security using identity-based cryptography”, Lecture Notes in Comput. Sci., vol 5061, pp. 482–489, 2008.
[10] J. Munilla, A.Ortiz, and A. Peinado, “What can RFID do for VANETs? A Cryptographic point of view”, International Conference on Security and Cryptography (SECRYPT 2010), pp. 295–298, 2010.
[11] National Institute of Standard and Technology, “Digital Signature Standard (DSS)”, Federal Information Processing Standard Publication, FIPS 186-3, 2009.
[12] National Institute of Standard and Technology, “(AES)”, Federal Information Processing Standard Publication, FIPS 197, 2001.
[13] QR-Codes, http://www.denso-dave.com/qrcode/qrstandard-e.hmtl
[14] Quickmark Encrypted QR Code, http://www.quickmark.com.tw
[15] R. Rivest, A. Shamir, and L.M. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems’ Commun. ACM, vol 21, no. 2, pp. 120–126, 1978.
[16] A. Shamir, “Identity-based cryptosystems and signature schemes”, Lecture Notes Comput. Sci., vol 196, pp. 47–53, 1984.
[17] Internet Mail Consortium, “vCard: The Electronic Business Card”, Version 2.1, 1996.
[18] J.F. Weng, “The study of RSA algorithm on QR code design”, Technical Report etd-0905108-095513, Computer Science and Engineering Department, Tatung University, Taiwan.