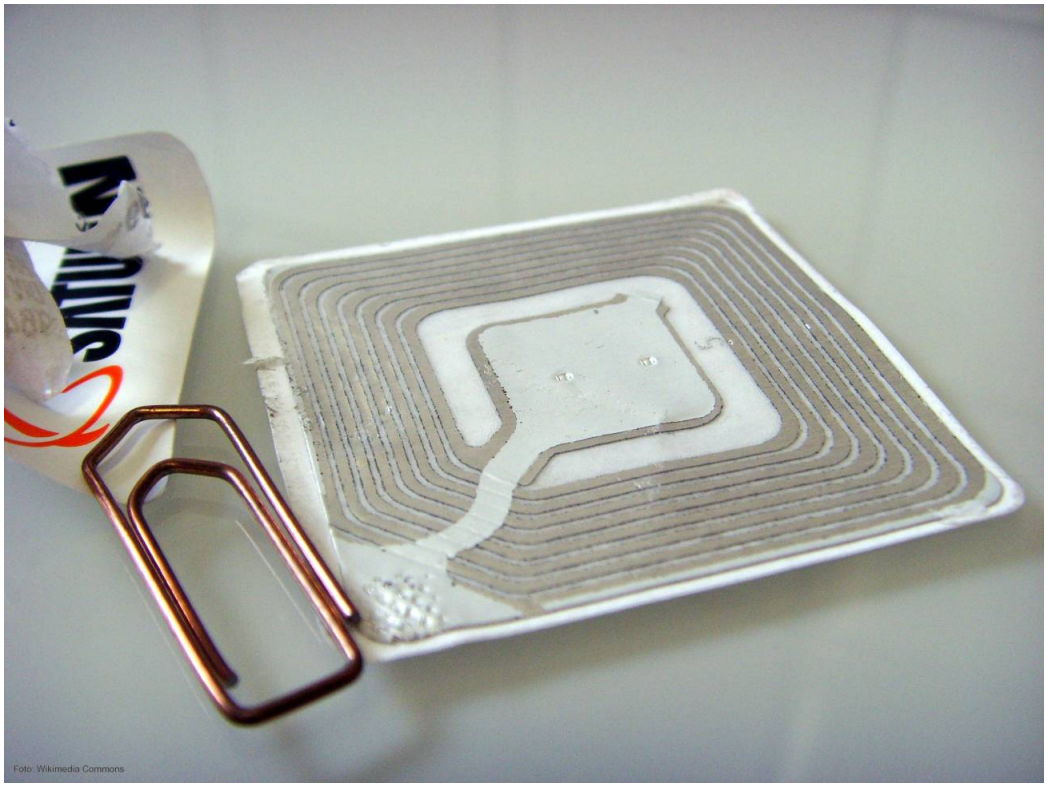
Cómo proteger y enviar la información digital

Comercio electrónico, uso del DNI electrónico, tarjetas de pago o los móviles son algunas de las aplicaciones en las que se requiere la mano de los expertos en matemática aplicada y álgebra. Un grupo de científicos de la Universidad de Valladolid investiga la información que nos llega o se almacena a través de estos canales para protegerla a través de la criptografía y corregir los errores que se producen al transmitir esa información.

DICYT 29/3/2011 14:01 CEST



Chip de RFID en el reverso de un código de barras. Foto: DiCYT.

Ambas líneas de investigación son las dos ramas principales en las que está trabajando actualmente el Grupo de Investigación Reconocido (GIR) Codificación de la Información y Criptografía. Aunque existen varios grupos en Criptografía en España, el de la Universidad de Valladolid está considerado uno de los pocos especializados en códigos correctores de

errores.

Como ha explicado a DiCYT Juan Tena, coordinador del Grupo, los códigos se utilizan en múltiples campos como los nuevos DNI o en los productos que se compran en el supermercado. Se trata de códigos detectores que pueden determinar si algo está mal, aunque en este caso no especifican de qué se trata.

“Si existe un error en un número o en la letra del DNI lo detectan, pero no saben en cuál se encuentra”, añade. Así, los códigos correctores de errores “tienen un código más fuerte que permite saber en qué cifra se ha producido el error”. Estos códigos, señala, son especialmente útiles en envíos a gran distancia “como las fotos enviadas desde Marte o las imágenes procedentes de satélite”.

Mensajes secretos cifrados

Entre las muchas investigaciones, trabajan en una de las ramas más “curiosas” de la criptografía, denominada esteganografía, utilizada para evitar las sospechas que provoca la información encriptada (mensajes cifrados). El objetivo de esta especialidad es transmitir la información sin que se vea y con medios inocuos.

En esta área está especializado el investigador del grupo Carlos Munuera, que explica cómo este tipo de criptografía “se ha usado en los envíos de mensajes secretos emitidos por Ben Laden a través de Internet, con la utilización de fotografías que contenían información secreta en algunos píxeles de la imagen”. Es un método que cuenta con más de 2.000 años de antigüedad y que fue utilizado en un principio para las operaciones militares y de guerra.

Códigos para redes de comunicación

Otro de sus campos son los códigos para redes, en el que trabaja la profesora Ángela Barbero, integrante también del grupo, que investiga cómo varias fuentes y receptores pueden enviar y recibir, respectivamente, la mayor información posible a través de nodos intermedios. Este campo de investigación es muy reciente y la primera vez que se habló de que los nodos

intermedios pudieran combinar la información y no sólo copiarla y retransmitirla fue en 2000.

Este tipo de códigos se utilizan actualmente en comunicaciones a través de redes inalámbricas (como las redes de satélites) o en la distribución y compartición de ficheros P2P (como la aplicación Avalanche de Microsoft), entre otras aplicaciones en las que la información proviene de muchas fuentes y ha de ser enviada a numerosos destinos de la forma más eficiente posible.

Por su parte, otros dos integrantes del grupo, Javier Galán y Edgar Martínez investigan otra especialidad de los códigos correctores de errores, los códigos aritméticos, que se utilizan en los procesadores aritméticos de las computadoras para detectar precisamente los errores aritméticos.

Mensajes cifrados para ordenadores cuánticos

Además, actualmente Martínez está encaminando sus investigaciones a estudiar los sistemas de encriptado que podrán soportar los futuros ordenadores cuánticos, cuya capacidad les permitirá realizar muchas operaciones en paralelo. Uno de estos sistemas, el diseñado por McEliece, es el objetivo del trabajo de Edgar Martínez y la becaria Irene Márquez, para determinar si podría ser utilizado en estos ordenadores futuristas sin sufrir daños.

En esta línea Juan Tena recuerda que, con los futuros ordenadores cuánticos “la mayor parte de los sistemas de seguridad actuales no valdrían”. Aunque aún queda tiempo para que este tipo de ordenadores sean habituales los investigadores señalan que, sabiendo lo que puede pasar con ellos, “conviene estar preparados”. “Ya se sabe que algunos de los sistemas de seguridad que se usan hoy se destruirían y en cambio a otros no los atacaría o sólo lo haría a medias, mientras que otros son más resistentes”, concluye.

Juan Tena, Francisca Blanco y Javier Galán centran su trabajo en Criptografía elíptica y firmas digitales con curvas elípticas, o lo que es lo mismo, trabajan en el desarrollo de sistemas criptográficos que admitan claves más pequeñas. Esto permite mejorar la seguridad de los sistemas, ya que ésta radica en la fortaleza de las claves.

TAGS | CRIPTOGRAFÍA | CHIP | RFID