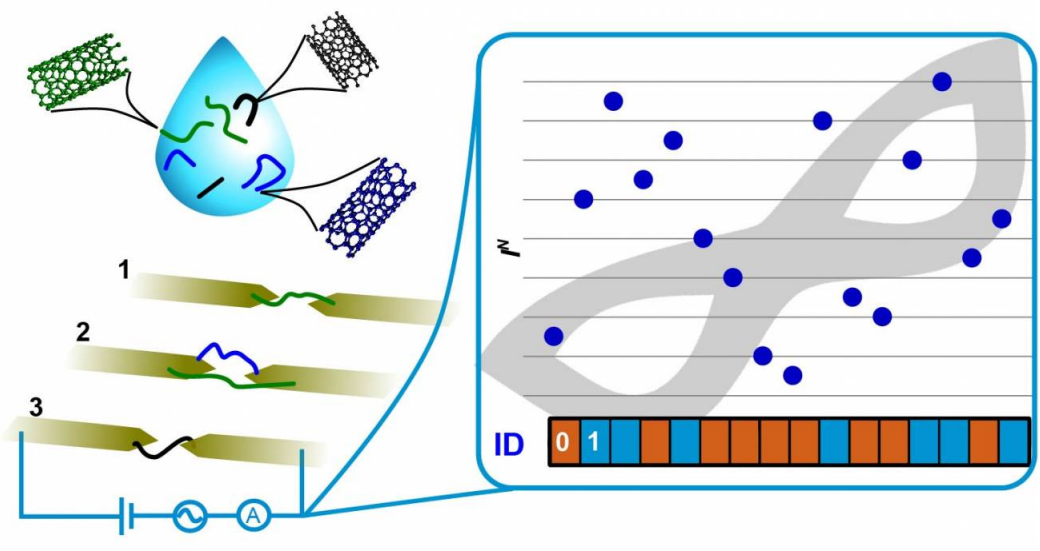
Nanotubos de carbono para autentificar información y combatir falsificaciones

Investigadores de IMDEA Nanociencia han desarrollado una función físicamente no clonable (PUF, por sus siglas en inglés) basada en nanotubos de carbono para su aplicación en sistemas antifraude incorporados en circuitos electrónicos. Se trata de nanodispositivos con un patrón de conductancia único, extraordinariamente difícil de duplicar, que se puede traducir en bits de información.

SINC 21/5/2019 09:00 CEST



Esquema de funciones físicamente no clonables basadas en nanotubos de carbono. / Enrique Burzurí

La ubicuidad de los dispositivos electrónicos hace imprescindible el uso de herramientas de encriptación y antifalsificación para proteger la privacidad y seguridad de los usuarios. Con la creciente expansión del internet de las cosas, la protección frente a ataques que vulneren la autenticidad de los productos se hace cada vez más necesaria.

Para proteger los mensajes, tradicionalmente se han usado diferentes sistemas: contraseñas, firmas digitales o cifrado. Esta criptografía se basa en claves que desconoce un posible atacante, pero desafortunadamente estos sistemas van quedándose obsoletos a medida que aparecen nuevos

ataques más invasivos: *malware*, los llamados ataques API (interfaz de programación de aplicaciones) o directamente ataques físicos al hardware.

> Estos dispositivos con nanotubos de carbono son fácilmente medibles y proporcionan un patrón de conductancia intrínseco muy difícil de duplicar

En este contexto, y mientras la computación cuántica avanza lentamente hacia el paradigma criptográfico, ser presentan las denominadas **funciones físicamente no clonables** (PUF, por sus siglas en inglés) como la opción para asegurar la identificación única y efectiva. Una PUF es un dispositivo que presenta unas propiedades físicas únicas y no repetibles que pueden traducirse en bits de información utilizables.

La idea de utilizar características físicas aleatorias para identificar sistemas o personas no es nueva. De hecho, la identificación de individuos mediante la huella dactilar se ha usado desde el siglo XIX. En la actualidad, la identidad de los dispositivos electrónicos ha podido establecerse utilizando PUF, que son “las huellas dactilares electrónicas” de un circuito integrado.

La autenticación basada en estos dispositivos comprende un chip fabricado mediante procesos intrínsecamente aleatorios que hacen casi imposible su clonación, aun cuando se conoce con precisión todos los detalles del proceso de fabricación. Las medidas de las diversas propiedades físicas del PUF dependen **de las propiedades a la nanoescala** del chip, y constituyen así una tecnología antifraude y antifalsificación muy potente. Para ser implementable a nivel industrial, el chip debe ser de bajo costo, escalable y sus propiedades deben ser fácilmente medibles mediante una función identificable.

Ahora, los investigadores Enrique Burzurí, Daniel Granados y Emilio M. Pérez de IMDEA Nanociencia proponen una ingeniosa y sencilla **función PUF basada en nanotubos de carbono**. Estos nanotubos se ensamblan (mediante dielectroforesis) a una serie de 16 electrodos, en los cuales se forman uniones aleatorias: en cada par de electrodos habrá uno, varios o ningún nanotubo.

Transformar un inconveniente en una gran ventaja

La medida de las curvas intensidad-voltaje proporciona un patrón único que es inherente a cada PUF y es casi imposible de reproducir. Esta nanotecnología explota una característica de los nanotubos de carbono que habitualmente ha sido un inconveniente para transformarla en su punto fuerte: la dificultad de conseguir nanotubos de carbono con idéntica quiralidad, es decir, con idénticas propiedades electrónicas (conductor o semiconductor). También, los defectos inherentes a la fabricación como son las vacantes o funcionalidades de oxígeno hacen que dos nanotubos de carbono con idéntica quiralidad no presenten la misma conductancia.

Se propone una medida de corriente sencilla, barata y fácilmente implantable en un circuito electrónico

Las PUF ideadas en IMDEA Nanociencia son dispositivos físicos **fácilmente medibles y que proporcionan un patrón de conductancia intrínseco** a cada uno de ellos extraordinariamente difícil de duplicar.

Dado una misma PUF, dos desafíos (*input*) diferentes producen respuestas diferentes, y dado un mismo desafío, dos PUF producen dos respuestas diferentes. De este modo, estos dispositivos basados en nanotubos de carbono pueden ser identificados por el valor de las respuestas que generan a desafíos concretos. Aquí no es válido cualquier desperfecto de la PUF: este debe ser medible y proporcionar una firma única del mismo.

En la actualidad existen diversos tipos de PUF que se basan en otras propiedades físicas como son la reflectividad o la anisotropía magnética. Sin embargo, la medida de corriente propuesta por los investigadores es **la más sencilla, barata** (un solo paso de litografía o proceso de impresión) **y la más fácilmente implantable en un circuito electrónico**, además de ser potencialmente escalable a un número mayor de electrodos para aumentar su complejidad.

Según los autores, estas nuevas PUF podrían implantarse en *smartphones*, microcontroladores, sensores inteligentes, actuadores y también podrían

usarse como firma digital.

Referencia bibliográfica:

Enrique Burzurí, Daniel Granados y Emilio M. Pérez. "Physically unclonable functions based on single-walled carbon nanotubes: a scalable and inexpensive method toward unique identifiers". *ACS Appl. Nano Mater.* 2019.

Investigación cofinanciada por la Comisión Europea (MSCA-IF y ERC), el Ministerio de Economía y Competitividad, la Comunidad de Madrid, así como el programa de Centros de Excelencia Severo Ochoa.

TAGS | NANOTUBOS DE CARBONO | ENCRIPTACIÓN | ANTIFRAUDE | ELECTRÓNICA |