SHAFRIRA GOLDWASSER, INVESTIGADORA DEL MIT Y PREMIO TURING ASISTENTE AL HEIDELBERG LAUREATE FORUM

“Me cuesta imaginar un mundo conectado por la comunicación cuántica”

Shafrira Goldwasser (1958, EE.UU.) es profesora de Ingeniería Electrónica y Ciencia Computacional en el Massachusetts Institute of Technology (MIT), y profesora de ciencias matemáticas en el Weizmann Institute of Science, en Israel. Entre sus muchos logros en las ciencias computacionales destaca la construcción de los fundamentos teóricos de la criptografía moderna. Estos trabajos, juntos al desarrollo de nuevos métodos para comprobar la validez de pruebas matemáticas dentro de la teoría de la complejidad, le hicieron merecedora del Premio Turing en 2012.

Ágata Timón 9/10/2013 14:13 CEST

Shafrira Goldwasser. / Weizmann Institute of Science

Junto a otros premiados con este galardón, la Medalla Fields y los premios Abel y Nevanlinna, Shafrira Goldwasser, forma parte del primer Heidelberg Laureate Forum, que reúne durante una semana a 200 jóvenes investigadores con estos líderes científicos, con el objetivo de transferir el conocimiento y la experiencia entre diferentes generaciones. Es la única mujer de los 40 'laureados'.

¿Cuál cree que es el papel de las Ciencias de Computación Teórica frente al resto de las ciencias?

Las ciencias computacionales están presentes en casi todas las otras ciencias. Muchos de los problemas son problemas computacionales, a veces de manera evidente y otras no. Procesos del cambio climático, de la física, de la biología... pueden ser estudiados como problemas de computación. El cuerpo humano es una computadora, en la que se desarrollan procesos complejos. La ciencias de computación teóricas pueden ayudar a modelar lo que está sucediendo de manera apropiada, para saber cuán rápido avanzan los procesos, o cómo modificar los resultados.

"El cuerpo humano es una computadora en la que se desarrollan procesos complejos"

Usted trabaja específicamente en criptografía, ¿cuales son los grandes retos de este campo?

En el pasado cuando hablábamos de encriptación hablábamos de privacidad: encriptación y desencriptación. Ahora estamos desarrollando la llamada criptografía funcional, que no desencripta todo el mensaje, solo ciertos trozos que responden a determinada búsqueda y mantiene en secreto el resto. Hay nuevos métodos que permiten operar sobre el mensaje encriptado, obtener el resultado que buscas, y con las claves solo desencriptar esta parte de la información.

¿Qué aplicaciones puede tener este nuevo método?

Por ejemplo en los sistemas de vigilancia. Ahora hay cámaras por todas

partes, y la vigilancia, que es necesaria en un sentido, es también un problema porque puede atentar contra la privacidad de las personas. Una solución podría ser que toda la información registrada en las cámaras fuera encriptada. Cuando alguien, por alguna razón concreta, necesitara cierta información contenida en el registro, se podría hacer ese procesado manteniendo la encriptación, y tendrás el resultado encriptado. Podrías encontrar a un sospechoso sin recibir ninguna otra información. También en el correo encriptado: un tercero podría tener la capacidad de saber si un mensaje recibido encriptado es spam, pero nada más.

Cual cree que es la situación de la criptografía hoy, ¿podemos decir que se ha conseguido un protocolo 100% seguro?

El nivel de inviolabilidad de las técnicas más avanzadas es muy alto. Si alguien pudiera romper estos códigos en un tiempo alcanzable significaría que habría encontrado la respuesta a grandes problemas abiertos de las matemáticas, que los científicos, desde los tiempos de Gauss, no han sabido resolver. Siempre es posible, y podría ser que alguien lo resuelva de manera más rápida, pero hoy en día creemos que es imposible.

"Una solución a los problemas de privacidad podría ser que toda la información registrada en las cámaras de seguridad fuera encriptada"

¿Cómo se relaciona la matemática con la ciencia computacional?

La teoría de números ha sido una grandísima inspiración para las ciencias computacionales. Por un lado, para la criptografía, porque hay muchos protocolos de seguridad basados en propiedades de los números, pero también en los métodos que usamos para diseñar los algoritmos: usar la aleatoriedad para reducir los errores, para acotar el tiempo de ejecución, etc. Un ejemplo muy conocido es uso de los números primos en el protocolo de clave pública RSA. Se basa en el hecho de que se pueden generar infinitos números primeros para hacer la encriptación.

¿Cómo se generan estos infinitos números primos?

Al final de los años setenta se ideó un método para hacerlo de una manera probabilística. Se utiliza un algoritmo que como resultado te da un número que, con alta probabilidad, es un primo. Después, el siguiente paso, en el que yo trabajé, consistía en eliminar la incertidumbre: si el algoritmo dice que cierto número es primo, es primo. Para ello desarrollamos el algoritmo 'Las Vegas', también usa aleatoriedad, que afecta solamente al tiempo que está corriendo el algoritmo, pero no hay error en el resultado final. El problema es que hay una pequeña oportunidad de que tarde mucho, que no sea eficiente. Alrededor del 2005 tres compañeros indios desarrollaron un algoritmo de primalidad que resolvía el problema en un tiempo polinomial, no contiene aleatoriedad, es siempre rápido, siempre correcto.

"Cuando iba al instituto era buena en matemáticas, pero no estaba especialmente interesada en el campo, de hecho quería ser escritora"

¿Qué importancia cree que tendrá la teoría cuántica en la criptografía en el futuro?

Creo que es una dirección muy interesante, ya que la seguridad basada en la teoría cuántica se basa en principios, que no pueden reducirse a problemas matemáticos, que potencialmente podrían ser resueltos. Pero en este momento todavía no lo veo posible porque el tipo de equipo necesario para transmitir y recibir señales cuánticas es muy sofisticado, y de hecho no existe todavía. Me cuesta imaginar cómo el mundo podría estar contactado de esta manera. Pero en términos teóricos es fascinante.

Usted es la única mujer del grupo de los laureados del congreso, ¿cree que en las próximas ediciones mejorará esta situación?

En ciencias de la computación teóricas la situación está sin dudas mejorando, hay muy buenas mujeres en campos importantes, y tendremos que ver si conseguirán premios o no en los próximos años; yo creo que es posible. Tampoco sé bien cual es la razón: ¿las mujeres están en las listas y no las escogen, o es que no hay mujeres en las listas? Puede ser que las

mujeres no estén interesadas.

¿Cómo podría cambiar esto?

Creo que es importante que haya mujeres en los puestos de poder: en el grupo de computación teórica del MIT hay tres mujeres con posiciones permanentes. No es así en todos los sitios, aunque me gustaría que así fuera.

¿Cómo llegó usted a las ciencias de la computación?

Cuando iba al instituto era buena en matemáticas, pero no estaba especialmente interesada en el campo, de hecho quería ser escritora. Por una serie de coincidencias empecé a estudiar Computación, primero en la Universidad de Carnegie Mellon y luego en Berkeley, aunque nunca había programado antes. Allí conocí a Manuel Blum (premio Turing de1995), y me dio una clase fascinante sobre el problema de jugar a cara o cruz a través del teléfono. Uno de los interlocutores tira la moneda y el segundo tiene que adivinar si es cara cruz, teniendo la certeza de que el resultado no es manipulado. Requiere un protocolo criptográfico sencillo, pero me fascinó. Así empecé con la criptografía. Esos años en Berkeley fueron realmente fructíferos, llevamos la computación a problemas reales, emulando fenómenos del mundo real.

Derechos: **Creative Commons**

TAGS: HEIDELBERG | ENCRIPTACIÓN | PRIVACIDAD | MATEMÁTICAS | CRIPTOGRAFÍA | COMPUTACIÓN | MIT | CUÁNTICA |

Creative Commons 4.0
Puedes copiar, difundir y transformar los contenidos de SINC. Lee las condiciones de nuestra licencia

La ciencia es noticia