Rueda de prensa de los tres investigadores del MIT galardonados con el Premio Fronteras del Conocimiento en Tecnologías de la Información y la Comunicación

Goldwasser, Micali y Rivest analizan el reto de proteger la seguridad de los ciudadanos en la sociedad digital sin comprometer su intimidad

- El trabajo de estos matemáticos ha sentado las bases del campo de la criptografía, con un impacto enorme en múltiples aspectos de nuestra vida cotidiana en la era digital: desde el uso del correo electrónico o las redes sociales, hasta las compras on-line o las transacciones financieras
- Goldwasser ha explicado que ya existen tecnologías eficaces para sacar el máximo partido de los datos biomédicos sin comprometer la intimidad de sus propietarios: "Varios hospitales pueden compartir información sobre qué tratamiento ha dado mejor resultado sin desvelar de qué paciente procede la información"
- Rivest ha puesto en duda la seguridad del voto electrónico: "Hoy en día lo más seguro son las papeletas de papel, no le recomendaría a nadie que enviara su voto a través de internet"
- Micali, experto en el análisis de criptomonedas como bitcoin, está convencido de su gran utilidad, pero a la vez considera que "muchas de las que existen ahora no son en absoluto seguras"

Madrid, 12 de junio de 2018.- La cuestión de hasta qué punto es posible preservar la seguridad de los ciudadanos sin comprometer su intimidad no tiene una respuesta clara, ni siquiera para los principales expertos mundiales en criptografía. Shafi Goldwasser, Silvio Micali y Ronald Rivest, los tres investigadores galardonados con el Premio Fronteras del Conocimiento en la categoría de Tecnologías de la Información y la Comunicación, junto con su colega israelí Adi Shamir, debatieron intensamente esta mañana durante la rueda de prensa previa a la ceremonia de entrega de los galardones, que tendrá lugar mañana en la Fundación BBVA. Los tres galardonados son catedráticos en el Instituto Tecnológico de Massachusetts (MIT), en EEUU. El jurado de los premios se ha

referido a ellos informalmente como "guardianes de la confidencialidad en la era digital".

Para Goldwasser y Micali, la criptografía ofrece soluciones que permiten proteger los propios datos y a la vez que las fuerzas de seguridad puedan acceder a ellos en situaciones muy específicas, con el objetivo de actuar, por ejemplo, contra una organización terrorista. "No soy tan optimista", dijo en cambio Rivest, quien aseguró que "este es un debate muy activo que sigue abierto porque el problema es global y complejo, y no veo sobre la mesa soluciones que hagan posible desencriptar mensajes para atrapar criminales sin comprometer la intimidad de todos; nos falta mucho para conseguirlo".

Goldwasser puso ejemplos: "Hay herramientas matemáticas que hacen posible que la policía acceda a mi clave [para descifrar mi información encriptada] en determinadas circunstancias", por ejemplo si el mensaje cifrado en cuestión es una foto y en ella aparece un reconocido terrorista. La clave podría incluso estar fragmentada y sus componentes distribuidos en instituciones de confianza, de forma que solo en determinados casos pudiera reconstituirse, explicó Micali. Sin embargo, sus argumentos no terminaron de convencer a Rivest: "Podríamos seguir y seguir con este debate…"

El Premio Fronteras del Conocimiento se les ha concedido por sus "contribuciones fundamentales a la criptología moderna, un área con un tremendo impacto en nuestra vida cotidiana", señala el acta del jurado. Sus investigaciones "han hecho posible la transmisión segura de información electrónica, en ámbitos que abarcan desde el correo electrónico hasta las transacciones financieras. Su trabajo ha sentado además las bases de desarrollos como la firma digital, la tecnología blockchain y las criptomonedas", como el Bitcoin.

Rivest se mostró conservador también en el área a la que más esfuerzo le ha dedicado últimamente: la seguridad del voto electrónico. "Tendemos a pensar que la última tecnología es la mejor, pero en lo que se refiere a las elecciones, la última tecnología aún no es lo bastante segura", dijo Rivest. "Hoy en día lo más seguro son las papeletas de papel, no le recomendaría a nadie que enviara su voto a través de internet".

Goldwasser ha explicado sus últimas investigaciones, centradas en el objetivo de sacar el máximo partido de los datos sin comprometer la intimidad de sus propietarios. El objetivo es permitir que diferentes entidades compartan sus bases de datos para extraer la máxima información fruto de esa agregación, pero sin dar acceso a la identidad anidada en los datos. Esto es útil en multitud de ámbitos, por ejemplo en la biomedicina con el análisis de datos genómicos, o en la clínica: "Varios hospitales pueden compartir información sobre qué tratamiento ha dado mejor resultado sin desvelar de qué paciente procede la información", explicó.

Micali, por su parte, ha dedicado estos años al análisis de las criptomonedas. Está convencido de su gran utilidad, pero a la vez considera que "muchas de las que existen ahora no son en absoluto seguras". Él trabaja en una nueva plataforma de transacciones con su compañía Algorand. Según Micali, Algorand resuelve los que en su opinión son los principales defectos de Bitcoin y el resto de las criptomonedas en uso, entre ellos un exceso de consumo energético y la alta centralización de la emisión de monedas.

Los pioneros de la criptografía moderna

A finales de los años setenta, prácticamente solo los gobiernos manejaban información encriptada. En 1977 Rivest, Shamir y su colega en el MIT Len Adleman –que posteriormente abandonaría el área de la criptografía– idearon un algoritmo matemático que por primera vez ponía al alcance de todos la posibilidad de encriptar información. Lo bautizaron con sus iniciales, RSA, y antes de publicarlo en una revista especializada explicaron parte del trabajo en *Scientific American*, ofreciendo mandar el resto a quienes lo solicitaran. La NSA (Agencia Nacional de Seguridad estadounidense) intentó frenar la difusión del algoritmo en vano: sus autores recibieron 7.000 peticiones y la técnica RSA se convirtió en el pistoletazo de salida de la criptografía moderna. El uso de RSA, sobre todo combinado con otras técnicas, sigue estando hoy muy extendido.

Desde entonces Rivest y Shamir han seguido contribuyendo muy activamente a diferentes aspectos de la criptografía. Rivest ha creado un algoritmo ampliamente usado para comprobar que un determinado archivo –por ejemplo descargado de la web– no ha sido modificado.

Goldwasser y Micali eran ambos estudiantes cuando se creó RSA. El área de la criptografía les fascinó y su primera aportación, aún como estudiantes de doctorado, fue desarrollar la demostración matemática de que un determinado método de encriptación es de verdad indescifrable.

Tras esas contribuciones seminales han llegado muchas otras. Goldwasser y Micali desarrollaron la llamada 'prueba de conocimiento cero', que demuestra que es posible convencer al interlocutor de la veracidad de algo, sin mostrar ese algo. Se trata de un algoritmo esencial presente desde en los procesos de autenticación, hasta en el uso de los bitcoins.

Biografías de los premiados

Shafi Goldwasser

Shafrira Goldwasser (Nueva York, Estados Unidos, 1958) se licenció en Matemáticas por la Universidad Carnegie Mellon y se doctoró en Ciencias de la Computación en la Universidad de California, Berkeley, con una tesis sobre teoría y práctica de la encriptación probabilística. En 1983 se incorporó al Instituto Tecnológico de Massachusetts y en 1995 ya era, además de catedrática, codirectora, junto con Ronald Rivest, del Grupo de Criptografía y

Seguridad de la Información. Desde 1997 es titular de la Cátedra RSA de Ingeniería Electrónica y Ciencias de la Computación, establecida ese mismo año por un acuerdo con RSA Data Security, la firma originalmente creada por Ronald Rivest, Adi Shamir y Leonard Adleman tras desarrollar el algoritmo al que dieron nombre.

En el Laboratorio de Ciencias de la Computación e Inteligencia Artificial del MIT es responsable del Grupo de Teoría de la Computación, además de codirectora del de Criptografía. Asimismo, y desde 1993, es catedrática de Ciencias de la Computación y Matemáticas Aplicadas en el Instituto Weizmann de Ciencia (Rehovot, Israel), donde forma parte del Grupo de Teoría.

Silvio Micali

Silvio Micali (Palermo, Italia, 1954) es licenciado en Matemáticas por la Universidad de La Sapienza (Roma) y doctor en Ciencias de la Computación por la Universidad de California en Berkeley. En 1983 se incorporó al MIT, donde hoy es catedrático y director asociado del Departamento de Ingeniería Electrónica y Ciencias de la Computación. Es, como Rivest y Goldwasser, miembro del Laboratorio de Ciencias de la Computación e Inteligencia Artificial de esta universidad.

Su investigación se centra en seguridad de la información: entre otras áreas ha trabajado, al igual que Adi Shamir, en 'prueba de conocimiento cero'; y ha sido distinguido junto con Shafi Goldwasser por su investigación en criptografía. Es autor de la obra Randomness and Computation (de la serie "Advances in Computing Research"), titular de 47 patentes y fundador de dos empresas: CoreStreet, dedicada al software de credenciales inteligentes -adquirida por ActiveIdentity en 2009) y Peppercoin, que creó con Ronald Rivest para explotar un sistema criptográfico de micropagos.

Ronald Rivest

Ronald Rivest (Schenectady, Estados Unidos, 1947) se licenció en Matemáticas en la Universidad de Yale y se doctoró en Ciencias de la Computación en la Universidad de Stanford. En 1974 se incorporó al Instituto Tecnológico de Massachusetts, donde hoy es Institute Professor -el rango más alto, que solo poseen catorce de los más de mil miembros del claustro- en el Departamento de Ingeniería Electrónica y Ciencias de la Computación.

Rivest es el fundador y actual codirector, junto con Goldwasser, del Grupo de Criptografía y Seguridad de la Información del Laboratorio de Ciencias de la Computación e Inteligencia Artificial del MIT. Es coautor de Introduction to Algorithms, manual universitario de referencia del área. Ha sido director de la Asociación Internacional de Investigación Criptológica y de la Asociación de Criptografía Financiera, y a lo largo de su trayectoria ha fundado tres compañías: RSA Data Security, Verisign -que se convirtió en la mayor autoridad de certificación de la encriptación y autenticación en internet- y de Peppercoin, esta última con Silvio Micali.

Más información

Toda la información biográfica de los premiados, así como los detalles de su contribución, entrevistas en vídeo y los audios de las ruedas de prensa en las que se dieron a conocer los fallos, con las primeras declaraciones de los premiados, están disponibles en la web de los Premios Fronteras del Conocimiento: https://www.premiosfronterasdelconocimiento.es/

Fundación BBVA

Para más información, puede ponerse en contacto con el Departamento de Comunicación de la Fundación BBVA (91 374 52 10; 91 374 31 39 y 91 374 81 73 o comunicacion@fbbva.es) o consultar en la web www.fbbva.es