Premio Fundación BBVA Fronteras del Conocimiento en Tecnologías de la Información y la Comunicación

La Fundación BBVA premia a Goldwasser, Micali, Rivest y Shamir por hacer posible una sociedad digital segura gracias a la criptografía moderna

- Los cuatro matemáticos han sentado las bases y ampliado el 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
- Sus algoritmos y protocolos de seguridad han dado lugar a aplicaciones en la autenticación de usuarios a través de claves de acceso, la firma digital, el voto electrónico o las criptomonedas como el Bitcoin
- "El trabajo agregado de los premiados es crucial para el tejido de nuestra sociedad digital conectada. Sus notables logros demuestran cómo la investigación teórica impulsa las aplicaciones prácticas en las tecnologías de la información y la comunicación que marcan nuestra vida cotidiana", señala el jurado que les ha concedido el premio

Madrid, 16 de enero de 2018.- El Premio Fundación BBVA Fronteras del Conocimiento en la categoría de Tecnologías de la Información y la Comunicación, en su décima edición, ha sido concedido a Shafi Goldwasser, Silvio Micali, Ronald Rivest y Adi Shamir por sus "contribuciones fundamentales a la criptología moderna, un área con un tremendo impacto en nuestra vida cotidiana", señala el acta del jurado. Sus avanzadas 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.

Las aportaciones de Goldwasser, Micali, Rivest y Shamir "resultan cruciales en el tejido de nuestra sociedad digital conectada", prosigue el acta. "Cada vez que accedemos a las redes sociales, hacemos compras on–line, votamos o firmamos electrónicamente recurrimos a la tecnología desarrollada a partir de su investigación".

Para el jurado, el despegue de la actual era digital simplemente no hubiera sido posible sin el desarrollo de técnicas que garantizan que el intercambio, uso y almacenamiento de la información se produce de forma segura. La criptografía es una tecnología "invisible" pero absolutamente indispensable en la sociedad moderna. A lo largo de las últimas cuatro décadas, los galardonados han sentado sus bases, y además han seguido ensanchando el campo con logros clave desde el aprovechamiento de las posibilidades de la gran cantidad de datos hoy disponibles -el *big data*- hasta el desarrollo tecnologías de gran potencial transformador, como las criptomonedas.

"Las sociedades humanas siempre han necesitado comunicaciones seguras", señala el acta, y esa necesidad se ha vuelto ahora más acuciante; por ello, "el diseño de protocolos abiertos de comunicación representa un gran desafío para la investigación al que han hecho frente admirablemente los galardonados".

En 1978, Adi Shamir y Ronald Rivest crearon junto a Leonard Adleman el algoritmo RSA (siglas que corresponden a sus apellidos), que fue "el primero de los protocolos seguros que definen la criptografía moderna", afirma el acta. RSA es un sistema de encriptación llamado 'de clave pública' porque cada interlocutor tiene dos claves: una pública, que se usa para encriptar el mensaje, y otra que solo conoce el receptor; el proceso de encriptación se basa en un problema matemático imposible de resolver con los ordenadores actuales –en este caso, la factorización de un número con muchos dígitos–, a menos que se tenga la clave personal. El uso de RSA, sobre todo combinado con otras técnicas, sigue siendo hoy muy extendido.

Shamir y Rivest, que hoy trabajan respectivamente en el Weizmann Institute, en Israel, y en el Instituto Tecnológico de Massachusetts (MIT), en EEUU, alcanzaron ese primer logro trabajando juntos, muy estrechamente, en el MIT. Desde entonces y durante cuarenta años han seguido contribuyendo muy activamente en diferentes aspectos de la criptografía.

Por entonces Goldwasser estudiaba en la Universidad de Carnegie Mellon (EEUU), y Micali en la Universidad La Sapienza, en Roma; poco más tarde, en 1982, ambos coincidirían como doctorandos en la Universidad de California en Berkeley (EEUU) e iniciarían una fructífera colaboración que, como primer gran resultado, acabaría sentando las bases teóricas del área. En concreto, ambos desarrollaron la demostración matemática de que un método de encriptación es de verdad indescifrable.

Como explicó ayer por teléfono Micali, "durante miles de años las personas han intentado encriptar mensajes, pero eran sistemas seguros solo hasta que un día dejaban de serlo porque alguien descifraba el código. RSA propuso un sistema de encriptación que nadie era capaz de romper, pero que tampoco nadie había demostrado que fuera indescifrable. Para demostrar que algo es seguro necesitas algo más, necesitas garantizar que ningún ataque futuro podría tener éxito. Nuestra contribución ha sido aplicar un método riguroso para asegurar

que si alguien quiere entender algo de un mensaje encriptado, tendría que resolver un problema matemático cuya resolución no se ha podido lograr durante siglos".

Tras esas contribuciones seminales, en colaboración e independientemente, Goldwasser y Micali "han ampliado el alcance de la criptografía más allá de su objetivo tradicional de garantizar la seguridad de las comunicaciones" -señala el acta- con desarrollos que han contribuido al florecimiento de la sociedad digital, al permitir colaborar y compartir información o realizar transacciones comerciales sin renunciar a la seguridad.

Por ejemplo, ambos han contribuido a desarrollar (junto a Charles Rackoff) la llamada 'prueba de conocimiento cero', que demuestra que es posible convencer al interlocutor de la veracidad de algo, pero sin mostrar ese algo. Se trata de un algoritmo esencial presente en un amplio abanico de aplicaciones desde los procesos de autenticación hasta el uso de los bitcoins. Los propios galardonados, en conversación telefónica tras conocer el fallo, pusieron ejemplos de la presencia de ese algoritmo: al entrar en una red social con una clave de acceso; al operar on-line en una cuenta bancaria; o al pagar con criptomonedas.

"Hoy realizamos on-line la mayor parte de las actividades que solíamos hacer en persona, y todo esto requiere la confianza del usuario que está transfiriendo dinero de una cuenta a otra, del comprador que está usando su tarjeta de crédito, o del usuario que está enviando un email. Para esto necesitamos técnicas de encriptación para prevenir el robo de identidad y la invasión de la privacidad, y lo conseguimos gracias a la criptografía", explica Goldwasser. "En nuestra vida cotidiana, cualquier 'password' que tecleamos, o cualquier firma digital que usamos, está protegida por técnicas basadas en nuestro trabajo", asegura Micali.

Goldwasser también destaca otro de sus logros, relevante para el aprovechamiento de la era del *big data*: cuando diferentes entidades ponen en común sus bases de datos para extraer la máxima información fruto de esa agregación, pero sin dar acceso a la identidad anidada en los datos. Es lo que ocurre, por ejemplo, cuando se comparten datos genómicos de la población.

Para Goldwasser, es importante que los ciudadanos sean conscientes de lo valiosos que son sus datos personales, y de que no deben proporcionarlos libremente. Recuerda, además, que las herramientas criptográficas actuales sí permiten hacer compatible la protección de la privacidad de los ciudadanos con la seguridad. Y comenta el gran potencial del área: "Existen métodos de criptografía eficaces que no se están utilizando todavía… Las empresas informáticas deberían trabajar más para construir sistemas que apliquen las ideas maravillosas que hemos desarrollado en el campo de la criptografía y que todavía no se han implementado".

Rivest y Shamir también han seguido haciendo valiosas contribuciones durante su carrera. Rivest ha creado, en concreto, un algoritmo ampliamente usado que permite comprobar que un determinado archivo –por ejemplo descargado de la web- no ha sido modificado. Shamir ha desarrollado el área del criptoanálisis diferencial, que se ocupa de cómo desencriptar códigos.

Ayer, tras conocer la concesión del premio, Rivest comentó los grandes cambios experimentados a lo largo de su carrera en la criptografía y, en paralelo, en la sociedad: "A finales de los años 70, ni siquiera existía la World Wide Web, así que era inimaginable pensar que nuestro método se convertiría en lo que es hoy... En la actualidad, cada vez que realizamos una compra 'online', la seguridad de la transacción está basada en nuestra tecnología de encriptación, y es gracias a ella que podemos confiar en que estamos hablando con Amazon, y viceversa".

Las tecnologías de bitcoin y blockchain (cadena de bloques) constituyen ahora uno de los focos de interés de estos cuatro expertos. Para Rivest, "Bitcoin es una tecnología interesante, pero la realidad es que existe mucha exageración en este terreno y todavía es muy pronto para saber si realmente se convertirá en un sistema fiable capaz de crear una nueva economía digital".

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.

Adi Shamir

Adi Shamir (Tel Aviv, Israel, 1952) se licenció en Matemáticas en la Universidad de Tel Aviv y se doctoró en el Instituto Weizmann de Ciencia en 1977. Tras un año en la Universidad de Warwick, fue Assistant Professor de Matemáticas en el MIT entre 1977 y 1980. Allí conoció a Ronald Rivest y Leonard Adleman, con quienes inventó el algoritmo RSA. Al terminar su estancia en el MIT, se incorporó al Instituto Weizmann (Rehovot, Israel), donde hoy es titular de la Cátedra Borman de Ciencias de la Computación.

Además del RSA, el Esquema de Shamir para la compartición de secretos y el criptoanálisis diferencial, el investigador israelí consiguió la ruptura del criptosistema de Merkle-Hellman, uno de los primeros sistemas de llave pública. Es además, creador de los dispositivos de factorización de enteros TWIRL y

TWINKLE, autor de la criptografía basada en la identidad e inventor de la criptografía visual, que se basa en romper una imagen -que puede ser un texto- de forma que las piezas resultantes parezcan imágenes aleatorias de píxeles blancos y negros.

Jurado y comisión técnica de Tecnologías de la Información y la Comunicación

El rigor, calidad e independencia del jurado ha situado estos galardones entre los más importantes del mundo y ha merecido la atención de la comunidad científica internacional.

El jurado de esta categoría ha estado presidido por **Georg Gottlob,** catedrático de Informática en la Universidad de Oxford (Reino Unido) y catedrático adjunto en Ciencias de la Computación en la Universidad Tecnológica de Viena (Austria), y ha contado con **Mario Piattini,** catedrático de Lenguajes y Sistemas Informáticos y director del Grupo de Investigación Alarcos de la Universidad de Castilla-La Mancha, como secretario. Los vocales han sido **Regina Barzilay,** catedrática Delta Electronics del departamento de Ingeniería Electrónica y Ciencias de la Computación del MIT, el Instituto Tecnológico de Massachusetts (Estados Unidos); **Liz Burd,** vicerrectora de Aprendizaje y Enseñanza en la Universidad de Newcastle (Australia); **Ron Ho,** director sénior de Ingeniería del Grupo de Soluciones Programables en Intel; **Rudolf Kruse,** catedrático emérito de la Facultad de Ciencias de la Computación en la Universidad de Magdeburg (Alemania); y **Joos Vandewalle,** presidente de la Real Academia Flamenca de Ciencias y Artes de Bélgica y catedrático emérito del Departamento de Ingeniería Eléctrica (ESAT) de la Universidad Católica de Lovaina (Bélgica).

En cuanto a la **comisión técnica del CSIC**, ha estado coordinada por **Mª Victoria Moreno,** vicepresidenta adjunta de Áreas Científico-Técnicas del Consejo Superior de Investigaciones Científicas, y ha estado compuesta por **Carmen García,** profesora de investigación y coordinadora del Área de Ciencia y Tecnologías Físicas en el Instituto de Física Corpuscular (IFIC); **Roberta Zambrini**, científica titular en el Instituto de Física Interdisciplinar y Sistemas Complejos (IFISC); **Federico Thomas**, profesor de investigación en el Instituto de Robótica e Informática Industrial (IRII); **Juan Antonio Rodriguez,** científico titular en el Instituto de Investigación en Inteligencia Artificial (IIIA); y **Ángela Ribeiro,** científica titular en el Centro de Automática y Robótica (CAR).

Sobre los Premios Fundación BBVA Fronteras del Conocimiento

El impulso del conocimiento basado en la investigación y la creación artística y cultural, y la interacción entre ambos dominios, constituyen el núcleo del programa de trabajo de la **Fundación BBVA**, así como el reconocimiento del talento y la excelencia en un amplio abanico de disciplinas, desde la ciencia a las humanidades y las artes.

Con esos objetivos como guía, en el año 2008 se crearon los **Premios Fundación BBVA Fronteras del Conocimiento** para reconocer contribuciones particularmente significativas en un amplio espectro de áreas científicas, tecnológicas y artísticas, así como respuestas basadas en el conocimiento a retos centrales del siglo XXI. Las áreas abarcadas por los Premios Fronteras del Conocimiento responden al mapa del conocimiento actual, tanto por las disciplinas contempladas como por atender a la interacción entre ellas en campos interdisciplinares.

Las **ocho categorías** incluyen áreas clásicas como las *Ciencias Básicas (Física, Química y Matemáticas)* y otras más recientes como la *Biomedicina;* algunas de ellas características de nuestro tiempo -*Tecnologías de la Información y la Comunicación, Ecología y Biología de la Conservación, Cambio Climático, Economía, Finanzas y Gestión de Empresas, y Cooperación al Desarrollo;* y un área particularmente innovadora de las artes, *Música Contemporánea*.

En la evaluación de las nominaciones a los premios, procedentes de numerosas instituciones y países, la Fundación BBVA cuenta con la colaboración de la principal entidad pública española de investigación, el **Consejo Superior de Investigaciones Científicas (CSIC)**. El CSIC designa Comisiones Técnicas de Evaluación, que llevan a cabo una primera valoración de las candidaturas y, posteriormente, elevan al jurado una propuesta razonada de finalistas. El CSIC designa también la Presidencia de cada uno de los jurados.

CALENDARIO DE RUEDAS DE PRENSA PARA ANUNCIO DE LOS PRÓXIMOS GALARDONADOS

Ciencias Básicas	Martes, 23 de enero de 2018
Biomedicina	Martes, 30 de enero de 2018
Ecología y Biología de la Conservación	Martes, 6 de febrero de 2018
Música Contemporánea	Miércoles, 14 de febrero de 2018
Economía, Finanzas y Gestión de Empresas	Martes, 20 de febrero de 2018
Cooperación al Desarrollo	Martes, 27 de febrero de 2018

PRIMERAS DECLARACIONES E IMÁGENES DEL PREMIADO

Pueden acceder a un vídeo con la primera entrevista al premiado tras recibir la noticia del galardón en el servidor FTP de Atlas con las siguientes coordenadas:

Servidor: **5.40.40.61**

Usuario: **AgenciaAtlas4**

Contraseña: **mediaset17**

El vídeo lleva por nombre:

"PREMIO TIC"

En caso de incidencia pueden contactar con **Miguel Gil** de la productora Atlas:

Móvil: 619 30 87 74

E-Mail: mgil@mediaset.es

Fundación BBVA

Para más información, póngase en contacto con el Departamento de Comunicación y Relaciones Institucionales 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