Nota de prensa
3 de marzo de 2020

La Fundación BBVA premia a Charles Bennett, Gilles Brassard y Peter Shor por su papel fundamental en el desarrollo de la computación y la criptografía cuánticas

- En los años ochenta, el físico químico Bennett y el informático Brassard inventaron la criptografía cuántica, que "permite codificar y transmitir mensajes usando las leyes de la física cuántica de manera que impide la escucha de terceros", según el acta del jurado
- La trascendencia de esta tecnología se demostró diez años después, cuando el matemático Shor descubrió que un hipotético ordenador cuántico convertiría en inservibles los sistemas de criptografía convencional en los que se basan la seguridad y la privacidad de las comunicaciones actuales en internet
- Sus contribuciones pioneras han dado un gran impulso al desarrollo de futuros ordenadores cuánticos que prometen realizar operaciones de cálculo a una velocidad y escala mucho mayor que los ordenadores actuales, así como de sistemas criptográficos que puedan garantizar la inviolabilidad de las comunicaciones

El Premio Fundación BBVA Fronteras del Conocimiento en la categoría de Ciencias Básicas ha sido concedido en su duodécima edición a Charles Bennett, Gilles Brassard y Peter Shor por sus "contribuciones sobresalientes a las áreas de la computación y la comunicación cuánticas", afirma el acta del jurado.

Bennett y Brassard, físico químico e informático respectivamente, inventaron en los años ochenta la criptografía cuántica, que garantiza la inviolabilidad física de las comunicaciones. La importancia de su trabajo se hizo patente cuando diez años más tarde el matemático Peter Shor descubrió que un hipotético ordenador cuántico convertiría en inservibles los sistemas de criptografía convencional en los que se basan la seguridad y la privacidad de las comunicaciones actuales en internet.

3 de marzo de 2020

El jurado, presidido por el premio Nobel de Física Theodor Hänsch y cuyo secretario es el físico cuántico Ignacio Cirac, ha destacado el gran impulso experimentado en los últimos años por las tecnologías cuánticas, que se asienta en gran medida sobre las aportaciones pioneras de los galardonados. Su trabajo –describe el acta– "abarca múltiples disciplinas y aúna conceptos de matemáticas, física y ciencias de la computación. Sus ideas están jugando un papel clave en el desarrollo de las tecnologías cuánticas para la comunicación y la computación".

La invención de la criptografía cuántica

La criptografía cuántica nació como un hallazgo proveniente de la ciencia básica que en unas décadas ha dado lugar a una nueva tecnología ya en el mercado, y en pleno auge.

Cuando Bennett, investigador en IBM Research desde hace más de cuatro décadas, y Brassard, actualmente catedrático en Ciencia de la Información Cuántica en la Universidad de Montreal, empezaron a colaborar, en 1979, ese escenario estaba muy lejos de ser siquiera imaginable. La física cuántica y la computación eran campos de trabajo distantes entre sí, y la investigación en la relación entre ambos se consideraba marginal. Para 1983, no obstante, Bennett y Brassard habían dado con un resultado muy llamativo: un sistema de criptografía que, según explica el acta del jurado, "permite codificar y transmitir mensajes usando las leyes de la física cuántica de manera que impide la escucha de terceros incluso si dispusieran de recursos computacionales cuánticos".

Para crear la criptografía cuántica, Bennett y Brassard aprovecharon uno de los extraños fenómenos que se dan en el mundo cuántico, la superposición, que –dicho de manera simplificada– hace posible que una partícula esté en dos o más lugares a la vez. La teoría cuántica prevé que si alguien observa la partícula esta duplicidad desaparece, y la partícula aparece en una posición o en la otra. Si esta partícula estuviera siendo transmitida, cualquier intento de *hackeo* rompería la superposición y los interlocutores lo sabrían.

Bennett y Brassard presentaron esta invención en un trabajo hoy conocido simplemente como BB84, por las iniciales de sus autores y el año de publicación. Se reconoce hoy como la primera aplicación práctica de la ciencia de la información cuántica.

"La información cuántica es un tipo de información que se altera si alguien la observa, y no puede ser copiada. Gilles Brassard y yo nos dimos cuenta de que podía tener una utilidad práctica: un sistema para enviar mensajes, en el que el emisor y el receptor advertirían de

inmediato si alguien hubiera escuchado el mensaje durante su transmisión", explicó ayer Bennett por teléfono tras conocer el fallo. "Eso es en esencia la criptografía cuántica".

La importancia de BB84 no fue reconocida por la comunidad de manera inmediata. Las técnicas criptográficas en uso, que garantizan la seguridad de todas nuestras comunicaciones y transacciones en internet, están basadas en el hecho de que hay problemas matemáticos que los ordenadores no pueden resolver, y a mediados de los ochenta nada hacía suponer que dejaría de ser así. Pero una década más tarde la situación cambiaría, gracias al trabajo de Peter Shor.

El algoritmo que amenazó a la criptografía convencional

Shor, catedrático de matemáticas aplicadas en el Instituto Tecnológico de Massachusetts (MIT), descubrió que precisamente el problema irresoluble en que se basa la criptografía clásica, la factorización de grandes números –es decir, su descomposición en números primos–, sí estaría al alcance de un hipotético ordenador cuántico. Como señala el acta, "Shor descubrió que los ordenadores cuánticos podrían factorizar números enteros mucho más rápido que cualquier súperordenador, comprometiendo por tanto la seguridad de los sistemas criptográficos".

Esta aportación lleva el nombre de su descubridor: el algoritmo de Shor, y es uno de los algoritmos cuánticos que constituyen el lenguaje, ahora en pleno desarrollo, en que hablarán los futuros ordenadores cuánticos.

En palabras de Bennett, "cuando Shor descubrió que si se construyera un ordenador cuántico, sería capaz de derrotar a los actuales sistemas criptográficos, esto estimuló mucho la investigación, ya que los criptógrafos querían desarrollar sistemas más seguros que ni siquiera un ordenador cuántico pudiera romper. Y al mismo tiempo, empezó a interesar la idea de desarrollar ordenadores cuánticos para averiguar qué utilidad podrían tener, aparte de descifrar códigos".

Gilles Brassard también recordó ayer por teléfono esa etapa de su carrera: "Nosotros creamos el sistema BB84 diez años antes de que Shor descubriera que un ordenador cuántico pondría en riesgo toda la infraestructura criptográfica que protege las comunicaciones en internet. La importancia de nuestro trabajo se hizo mucho más evidente después de ese trabajo de Shor. Así que, tiene gracia, porque en 1984 la teoría cuántica llevó a la invención del sistema más seguro de transmisión de información, y diez años después la

misma teoría puso en duda todos los sistemas criptográficos desarrollados hasta entonces. El nuestro, por el contrario, permanecería inalterado".

Bennett y Brassard siguieron colaborando estrechamente varias décadas. También han trabajado con Shor, que ayer explicó así su aportación: "Los actuales sistemas criptográficos dependen de la factorización. Si pudieras factorizar números rápidamente, podrías romper los códigos de los actuales sistemas criptográficos. Lo que demostré es que un ordenador cuántico podría factorizar números grandes con bastante rapidez. Por supuesto, hasta ahora nadie ha construido un ordenador cuántico lo suficientemente grande como para factorizar grandes números, y probablemente pasarán años o décadas hasta que se consiga".

Poco después de crear su algoritmo, Shor obtuvo otro resultado esencial: la corrección de errores cuánticos, "un requisito primordial que permite la escalabilidad de los ordenadores cuánticos", señala el acta.

Los ordenadores cuánticos, por su propia naturaleza física, están expuestos a una gran cantidad de ruido, fuente de numerosos errores. Antes del resultado de Shor no se creía tecnológicamente posible superar el desafío de aislar los ordenadores cuánticos lo bastante como para eliminar los errores. Shor insufló esperanza en el área y propulsó su avance.

"Todo el mundo pensaba que no se podían corregir errores en un ordenador cuántico porque, en cuanto intentas medir un sistema cuántico, lo alteras, y por lo tanto si intentas medir un error para corregirlo, modificas e interrumpes la computación. Pero mi algoritmo demostró que es posible aislar el error, de tal manera que puedes corregirlo sin alterar la computación", explica Shor.

Las promesas de una tecnología en auge

La criptografía cuántica es actualmente una de las tecnologías cuánticas más avanzadas, con varias empresas en Europa y Estados Unidos. En China existe ya una conexión entre Beijing y Shanghai que empieza a usarse para aplicaciones comerciales, y en 2016 China lanzó un satélite para establecer un enlace experimental con Europa.

El desarrollo de la computación cuántica, sin embargo, es visto por los galardonados como un desafío a largo plazo que no dará respuesta inmediata a las altas expectativas generadas por los primeros prototipos presentados por grandes empresas tecnológicas: "Estoy encantado de que

hoy muchas personas inteligentes investiguen en este campo, porque en el pasado solo éramos media docena de personas, y el progreso era mucho más lento. Pero la gente tiene demasiada prisa por conocer su utilidad práctica, sobre todo si tenemos en cuenta que la información cuántica es de naturaleza muy frágil, requiere un hardware muy preciso y resistente al error, y a cualquier impacto del entorno. Supone desafíos para la ingeniería extremadamente complejos, no necesariamente imposibles de superar, pero sin duda tardaremos años en lograrlo".

Sin embargo, los premiados no dudan en ningún momento del potencial futuro de los ordenadores cuánticos. Para Brassard, "el siglo XIX fue la era de la máquina de vapor, el siglo XX fue la era de la Información y el siglo XXI será recordado como la Era Cuántica, la era en la que las tecnologías cuánticas desencadenarán todos los principales cambios que veremos en la sociedad, de una manera que hoy no podemos prever".

Shor, por su parte, considera que "se tardará entre 5 y 10 años en lograr que un ordenador cuántico pueda hacer algo que pueda considerarse mínimamente útil", pero está convencido de que con el tiempo se lograrán aplicaciones revolucionarias con estas máquinas, por ejemplo en el campo biomédico para facilitar la creación de nuevos fármacos: "Ahora mismo el comportamiento de las moléculas no se puede simular adecuadamente, pero los ordenadores cuánticos podrían lograrlo, y ayudarnos a diseñar nuevos medicamentos".

Biografías de los premiados

Charles H. Bennett (Nueva York, Estados Unidos, 1943) se graduó en Química en la Universidad Brandeis (Waltham, Massachusetts, Estados Unidos) en 1964 y se doctoró en Física Química en la Universidad de Harvard en 1971. En 1972 se incorporó a IBM Research, donde continúa en la actualidad. Entre 1984 y 1986 fue profesor visitante en el departamento de Ciencias Informáticas de la Universidad de Boston y, entre 1986 y 1987, investigador visitante en el MIT Lab de Ciencias Informáticas. Según Google Scholar, las publicaciones de Bennett se han citado en más de 78.000 ocasiones. Además de IBM Fellow desde 1995, es miembro de la Sociedad Americana de Física y de la Academia Nacional de Ciencias de Estados Unidos.

Gilles Brassard (Montreal, Canadá, 1955) se licenció en Ciencias Informáticas por la Universidad de Montreal en 1972, y en 1979 obtuvo el doctorado en Ciencia Computacional Teórica en la Universidad de Cornell. Desde 1988 es catedrático de la Universidad de Montreal, donde actualmente ostenta la Cátedra de Investigación de Canadá en Ciencia de la Información desde 2001. Entre otras distinciones, es Doctor Honoris Causa por la Escuela Politécnica Federal de Zúrich, por la Universidad de Ottawa y por la Universidad de la Suiza italiana. Es fundador y

director científico del centro interdisciplinario Institut transdisciplinaire d'information quantique y ha sido editor jefe del Journal of Cryptology.

Peter Shor (Nueva York, Estados Unidos, 1959) se licenció en Matemáticas en el Instituto Tecnológico de California en 1981 y se doctoró en el Instituto Tecnológico de Massachusetts en 1985. Tras un año de investigación posdoctoral en Caltech, trabajó durante una década en AT&T Bell Laboratories y, entre 1996 y 2003, en AT&T Shannon Labs. En 2003 se incorporó al Instituto Tecnológico de Massachusetts como titular de la cátedra Henry Adams Morss y Henry Adams Morss Jr. de Matemáticas Aplicadas, institución donde dirige, además, el Comité de Matemáticas Aplicadas. En sus casi 40 años de trayectoria investigadora ha publicado más de 170 artículos en revistas especializadas.

Jurado y Comité Técnico de Ciencias Básicas

El jurado de esta categoría ha estado presidido por Theodor Hänsch, director de la División de Espectroscopia Láser del Instituto Max Planck de Óptica Cuántica (Alemania), y premio Nobel de Física, y ha contado como secretario con Ignacio Cirac, director de la División Teórica del Instituto Max Planck de Óptica Cuántica y premio Fundación BBVA Fronteras del Conocimiento en Ciencias Básicas. Los vocales han sido Emmanuel Candes, titular de la Cátedra Barnum-Simons en Matemáticas y Estadística en la Universidad de Stanford (Estados Unidos); Nigel Hitchin, catedrático emérito Savilian de Geometría en la Universidad de Oxford (Reino Unido); Hongkun Park, titular de la Cátedra Mark Hyman Jr. de Química y catedrático de Física en la Universidad de Harvard (Estados Unidos); Martin Quack, director del Grupo de Cinética y Espectroscopia Molecular en el Laboratorio de Química Física de la Escuela Politécnica Federal (ETH) de Zúrich (Suiza); y Sandip Tiwari, titular de la Cátedra Charles N. Mellowes de Ingeniería en la Universidad de Cornell (Estados Unidos).

En cuanto al Comité Técnico de Apoyo del Consejo Superior de Investigaciones Científicas (CSIC), ha estado coordinado por M.ª Victoria Moreno, vicepresidenta adjunta de Áreas Científico-Técnicas del Consejo Superior de Investigaciones Científicas (CSIC), e integrado por Carmen García García, coordinadora adjunta del Área Global Materia y profesora de investigación en el Instituto de Física Corpuscular (IFIC); Berta Gómez-Lor Pérez, investigadora científica en el Instituto de Ciencias Materiales de Madrid (ICMM); José Luis de Miguel Antón, científico titular en el Instituto de Óptica Daza de Valdés (IO); Carlos Prieto de Castro, coordinador del Área Global Materia y profesor de investigación en el Instituto de Ciencias Materiales de Madrid (ICMM); y Germán Sierra Rodero, profesor de investigación en el Instituto de Física Teórica (IFT).

www.premiosfronterasdelconocimiento.es

3 de marzo de 2020

Sobre los Premios Fundación BBVA Fronteras del Conocimiento

La Fundación BBVA tiene como foco de su actividad el fomento de la investigación científica y la creación cultural de excelencia, así como el reconocimiento del talento.

Los Premios Fundación BBVA Fronteras del Conocimiento, creados en 2008, reconocen e incentivan contribuciones de singular impacto en diversos campos de la ciencia, la tecnología, las ciencias sociales y las humanidades, aportaciones que han evidenciado una especial capacidad de ampliar significativamente el ámbito de lo conocido, hacer emerger nuevos paradigmas y campos del conocimiento. Sus ocho categorías son expresión del mapa del conocimiento del siglo XXI, abarcando la investigación básica en Física, Química y Matemáticas, la Biología y la Biomedicina, las Tecnologías de la Información y la Comunicación, las Humanidades y las Ciencias sociales, la Economía, Finanzas y Gestión de Empresas, la Ecología y Biología de la Conservación, el Cambio climático y un área de las artes particularmente innovadora como la música. Cada una de sus ocho categorías está dotada con 400.000 euros, un diploma y un símbolo artístico.

En la evaluación de las nominaciones recibidas, procedentes de numerosas instituciones y países, la Fundación BBVA cuenta con la colaboración de la principal entidad pública española de investigación, el CSIC. La Fundación BBVA, de forma conjunta con el Consejo Superior de Investigaciones Científicas, designa Comités Técnicos de Apoyo que llevan a cabo una primera valoración de las candidaturas, elevando al jurado una propuesta razonada de finalistas. El CSIC designa también la presidencia de cada uno de los jurados, integrados todos ellos por especialistas de reconocido prestigio en el correspondiente campo.

XII Edición
Premios Fundación BBVA Fronteras del Conocimiento
BBVA Foundation Frontiers of Knowledge Awards
12th Edition

www.premiosfronterasdelconocimiento.es

3 de marzo de 2020

PRIMERAS DECLARACIONES E IMÁGENES DE LOS PREMIADOS

Puede acceder a una entrevista al premiado tras recibir la noticia del galardón en el siguiente FTP:

Servidor: 5.40.40.61 ||| Usuario: AgenciaAtlas4 ||| Contraseña: mediaset17

El vídeo se encontrará en la carpeta:

"**PREMIO** CIENCIAS BÁSICAS"

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

Móvil: 619 30 87 74 ||| E-Mail: mgil@mediaset.es

Calendario de ruedas de prensa para el anuncio de próximos galardonados

Economía, Finanzas y Gestión de Empresas	Martes, 17 de marzo de 2020
Música y Ópera	Martes, 31 de marzo de 2020
Humanidades y Ciencias Sociales	Miércoles, 15 de abril de 2020

CONTACTO:
Departamento de Comunicación y Relaciones Institucionales
Tel. 91 374 52 10 / 91 374 81 73 / 91 537 37 69
comunicacion@fbbva.esPara información adicional sobre la Fundación BBVA, puede visitar:
www.fbbva.es