Press release
3 March, 2020

The BBVA Foundation recognizes Charles H. Bennett, Gilles Brassard and Peter Shor for their fundamental role in the development of quantum computation and cryptography

- In the 1980s, chemical physicist Bennett and computer scientist Brassard invented quantum cryptography, a technology that "allows encoding and transmitting messages using the laws of quantum physics in a way that makes them unreadable to eavesdroppers," in the words of the award committee
- The importance of this technology was demonstrated ten years later, when mathematician Shor discovered that a hypothetical quantum computer would drive a hole through the conventional cryptographic systems that underpin the security and privacy of Internet communications
- Their landmark contributions have boosted the development of tomorrow's quantum computers, which promise to perform calculations at a far greater speed and scale than today's machines, and enabled cryptographic systems that guarantee the inviolability of communications

The BBVA Foundation Frontiers of Knowledge Award in Basic Sciences has gone in this twelfth edition to Charles Bennett, Gilles Brassard and Peter Shor for their "outstanding contributions to the field of quantum computation and communication," said the committee in its citation.

Bennett and Brassard, a chemical physicist and computer scientist respectively, invented quantum cryptography in the 1980s to ensure the physical inviolability of data communications. The importance of their work became apparent ten years later, when mathematician Peter Shor discovered that a hypothetical quantum computer would render effectively useless the conventional cryptography systems underpinning the privacy and security of today's Internet communications.

The award committee, chaired by Nobel Physics laureate Theodor Hänsch with quantum physicist Ignacio Cirac acting as its secretary, remarked on the leap forward in quantum

technologies witnessed in these last few years, an advance which draws heavily on the new laureates' pioneering contributions. Their work, says the committee, "spans multiple disciplines and brings together concepts from mathematics, physics and computer science. Their ideas are playing a key role in the development of quantum technologies for communication and computation."

The invention of quantum cryptography

Quantum cryptography emerged in the realm of basic science, but in a few decades has produced a whole new technology that is now commercially available and tipped as a rising market. In 1979, when Bennett –at IBM Research, where he remains today– and Brassard –at the Université de Montréal, where he is currently Canada Research Chair in Quantum Information Science–, began working together, there was not the least hint of this future scenario. Quantum physics and computer science were separate, even distant fields, and any work on the linkages between them was confined to the fringes of established research. Yet by 1983, Bennett and Brassard had come up with an intriguing result: a cryptographic system which, as the committee describes it, "allows encoding and transmitting messages using the laws of quantum physics in a way that makes them unreadable to eavesdroppers, even if they had quantum computational resources."

To create quantum cryptography, Bennett and Brassard made use of one of those strange phenomena of the quantum world: superposition, which, in simplified terms, makes it possible for a single particle to be in two or more places at once. Quantum theory holds that this dual state is lost as soon as somebody observes the particle, which will then appear in one position or the other. And if the same particle was in the midst of being transmitted, any attempted hack would collapse the superposition, alerting the interlocutors.

Bennett and Brassard's protocol, known as BB84 after its inventors and year of publication, is today generally acknowledged as the first practical application of the science of quantum information.

"Quantum information is a kind of information that is disturbed by observation and cannot be copied," explained Bennett on the phone yesterday after hearing of the award. "Gilles Brassard and I realized that it could be used for the practical purpose of sending messages, in such a way that the sender and receiver could tell immediately whether anyone had listened to the message en route. And that, in essence, is quantum key distribution or quantum cryptography."

The importance of BB84 was not immediately recognized by the scientific community. The cryptographic protocols now in use, which underpin the security of all our Internet communications and transactions, are based on the existence of mathematical problems that

computers cannot solve, and in the mid-1980s there was nothing to suggest that this might one day change. However ten years later change it did, thanks to the work of Peter Shor.

The algorithm that challenged classical cryptography

Shor, Professor of Applied Mathematics at MIT, discovered that the supposedly intractable problem on which standard cryptography was based, the prime factorization of large numbers – i.e. the decomposition of a large number into its prime factors – would be within the scope of a hypothetical quantum computer. As the citation states, "Shor discovered that quantum computers could factorize integers much faster than any supercomputer, therefore compromising the security of conventional cryptographic schemes."

Shor's algorithm, so named for its author, is now one of the quantum algorithms that comprise the fast developing language to be spoken by tomorrow's quantum computers.

"When Shor discovered that if you could build a quantum computer", explains Bennett, "it would defeat certain cryptographic systems in widespread use, that stimulated a lot more research, because the cryptographers wanted to find more secure systems that were harder to break. And at the same time other people wanted to build a better quantum computer to see what it could be used for besides code breaking."

In phone conversation, Gilles Brassard also recalled this time in his career: "We created the BB84 system ten years before Peter Shor discovered that quantum computers, if they could be built, would completely undermine the cryptographic infrastructure that protects Internet communications. The importance of our work became much more evident after Shor destroyed everything else. It's sort of funny, because in 1984 quantum theory led to the most secure confidentiality possible. And ten years later the same quantum theory challenged all the currently-deployed cryptographic systems to protect the Internet. Our quantum cryptography, on the other hand, remained unscathed."

Bennett and Brassard would go on working closely together for several decades. Both have also collaborated with Shor, who explains his own contribution as follows: "Current cryptographic systems depend on the difficulty of factoring numbers. If you could factor numbers quickly, you could break all the codes of today's systems. What I showed is that a quantum computer could factor large numbers fairly quickly. Of course nobody has actually built a big enough quantum computer to factor those numbers yet, and it will probably be years or decades before they do."

Shortly after devising his algorithm, Shor made another landmark contribution, known as quantum error correction; "an essential requirement," in the words of the committee. "for enabling and scaling quantum computations."

Press release
3 March, 2020

By their very nature, quantum computers are exposed to a large volume of noise, causing numerous errors. Before Shor's finding, it was not believed theoretically possible to isolate quantum computers to such an extent that errors could be eradicated. So Shor, in essence, gave hope to the field and propelled it forward.

"Everyone thought that you couldn't correct errors on quantum computers," recalls Shor, "because as soon as you try to measure a quantum system you disturb it. In other words, if you try to measure the error so as to correct it, you disturb it and computation is interrupted. My algorithm showed that you can isolate and fix the error and still preserve the computation".

The promise of a rising technology

Quantum cryptography is right now one of the most advanced branches of quantum technology, with several companies up and running in Europe and the United States. In China a quantum communication terrestrial system known as Backbone has been laid between Beijing and Shanghai is already being used for commercial applications, and in 2016 the country launched an experimental satellite link with Europe.

The laureates, however, view the development of quantum computation as essentially a long-term prospect, unlikely to immediately fulfill the expectations stoked by the prototypes of leading tech firms. As Bennett reflects, "I really welcome the number of smart people working in this field, because back in the days when there were only half a dozen of us it didn't progress. But I think people are too eager to know what it's going to be used for right away, especially considering that quantum information is very delicate. It requires very precise hardware resistant to error and well insulated from environmental influences. These are tough engineering problems. Not necessary impossible, but they are hard and will take years to achieve."

That said, they have no doubts about the future potential of quantum computers. For Brassard, "the 19th century was the era of steam power, the 20th century was the era of information, and the 21st century will go down in history as the quantum age, the age in which quantum technologies dominate all the changes occurring in society, in a way we cannot yet foresee."

Shor, meantime, believes that "it will be 5 or 10 years before a quantum computer can do anything approaching useful." With time, however, he is convinced that these machines will deliver revolutionary applications, in biomedicine, for instance: "At the moment, it takes enormous amounts of computer time to simulate the behavior of molecules, but quantum computers could achieve that, and help design new drugs."

Press release
3 March, 2020

Bio notes

Charles H. Bennett (New York, United States, 1943) graduated with a BA in Chemistry from Brandeis University (Waltham, Massachusetts, United States) in 1964 then went on to complete a PhD in Chemical Physics at Harvard in 1971. The following year he joined IBM Research, where he remains to this day. From 1984 to 1986 he was a Visiting Professor in the Computer Science Department at Boston University, and from 1986 to 1987 a Visiting Scientist at the MIT Computer Science Lab. His publications have a Google Scholar citation count of over 78,000. An IBM Fellow since 1995, he is also a member of the American Physical Society and the U.S. National Academy of Sciences.

Gilles Brassard (Montreal, Canada, 1955) graduated in Computer Science from Université de Montréal in 1972, and in 1979 earned a PhD in Theoretical Computer Science from Cornell University. That same year, he joined the faculty at Université de Montréal, where he is currently Canada Research Chair in Quantum Information Science. He is founder and Scientific Director of the Institut transdisciplinaire d'informatique quantique and a former editor-in-chief of *Journal of Cryptology*. Among other distinctions, he holds honorary doctorates from ETH Zurich, the University of Ottawa and Università della Svizzera italiana, he was elected Fellow of the Royal Society, and is Officer in the Order of Canada as well as the Ordre national du Québec.

Peter Shor (New York, United States, 1959) completed a BA in Mathematics at the California Institute of Technology in 1981 then went on to obtain a PhD in 1985 from the Massachusetts Institute of Technology. After a year as a postdoc at the Mathematical Sciences Research Institute, Berkeley, he joined AT&T Bell Laboratories, where he remained for ten years, then moved to AT&T Shannon Labs from 1996 to 2003. That year, he became Henry Adams Morss and Henry Adams Morss Jr. Professor of Applied Mathematics at the Massachusetts Institute of Technology, where he also chairs the Applied Mathematics Committee. In a research career of almost 40 years, he has had more than 170 papers published in specialist journals.

Basic Sciences committee and evaluation support panel

The committee in this category was chaired by Theodor Hänsch, Director of the Division of Laser Spectroscopy at the Max Planck Institute of Quantum Optics (Germany), and the 2005 Nobel Laureate in Physics, with Ignacio Cirac, Director of the Theory Division at the Max Planck Institute of Quantum Optics (Germany) acting as secretary. Remaining members were

Press release
3 March, 2020

Emmanuel Candes, the Barnum-Simons Chair in Mathematics and Statistics at Stanford University (United States); Nigel Hitchin, Emeritus Savilian Professor of Geometry at the University of Oxford (United Kingdom); Hongkun Park, Mark Hyman Jr. Professor of Chemistry and Professor of Physics at Harvard University (United States); Martin Quack, Head of the Molecular Kinetics and Spectroscopy Group at ETH Zurich (Switzerland); and Sandip Tiwari, Charles N. Mellowes Professor in Engineering at Cornell University (United States).

The evaluation support panel of the Spanish National Research Council (CSIC) was coordinated by María Victoria Moreno, Deputy Vice President for Scientific and Technical Areas, and formed by: Carmen García García, Deputy Coordinator of the MATERIA Global Area and research professor at the Institute of Corpuscular Physics (IFIC); Berta Gómez-Lor Pérez, scientific researcher at the Institute of Materials Science of Madrid (ICMM); José Luis de Miguel Antón, tenured scientist at the Institute of Optics "Daza de Valdés" (IO); Carlos Prieto de Castro, Coordinator of the MATERIA Global Area and research professor at the Institute of Materials Science of Madrid (ICMM); and Germán Sierra Rodero, research professor at the Institute for Theoretical Physics (IFT).

About the BBVA Foundation Frontiers of Knowledge Awards

The BBVA Foundation centers its activity on the promotion of world-class scientific research and cultural creation, and the encouragement of talent.

The BBVA Foundation Frontiers of Knowledge Awards, established in 2008, recognize and reward contributions of singular impact in diverse fields of science, technology, social sciences and the humanities that have demonstrably expanded the frontiers of the known world, opening up new paradigms and knowledge fields. Their eight categories are reflective of the knowledge map of the 21st century, encompassing basic research in Physics, Chemistry and Mathematics, Biology and Biomedicine, Information and Communication Technologies, Humanities and Social Sciences, Economics, Finance and Management, Ecology and Conservation Biology, Climate Change, and, within the arts, the supremely creative realm of music.

The BBVA Foundation is aided in the evaluation process by the Spanish National Research Council (CSIC), the country's premier public research organization. The Foundation and CSIC jointly appoint the evaluation support panels charged with undertaking an initial assessment of the candidates proposed by numerous institutions across the world and drawing up a reasoned shortlist for the consideration of the award committees. CSIC is also responsible for designating the chair of each committee, formed by eminent authorities in the subject area.

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

www.frontiersofknowledgeawards-fbbva.es

Press release

3 March, 2020

LAUREATE'S FIRST DECLARATIONS AND IMAGES

A recording of the laureates' first interview on receiving news of the award is available from the following FTP:

Server: 5.40.40.61 ||| Username: AgenciaAtlas4 ||| Password: mediaset17

The video is in the folder labelled:

"**PREMIO** CIENCIAS BÁSICAS"

In the event of connection difficulties, please contact Miguel Gil at production company Atlas:

Mobile: 619 30 87 74 ||| E-mail: mgil@mediaset.es

Calendar of announcement events

Economics, Finance and Management	Tuesday, 17 March, 2020
Music and Opera	Tuesday, 31 March, 2020
Humanities and Social Sciences	Wednesday, 15 April, 2020

CONTACT:
Department of Communications and Institutional Relations
Tel. +34 91 374 5210 / 91 374 8173 / 91 537 3769
comunicacion@fbbva.es

For more information on the BBVA Foundation, visit: www.fbbva.es