**BBVA Foundation Frontiers of Knowledge Award in Information and Communication Technologies**

# The BBVA Foundation recognizes Goldwasser, Micali, Rivest and Shamir for enabling a secure digital society thanks to modern cryptography

- The four mathematicians have successively grounded and enlarged the field of cryptography, with ramifications in almost every area of our day-to-day lives in the digital era: from the use of e-mail or social networks to online shopping and financial transactions
- Their security protocols and algorithms underlie user authentication applications based on access keys, digital signatures, electronic voting systems and crypto-currencies such as Bitcoin
- "The aggregate work of the awardees is crucial to the fabric of our connected digital society," said the jury bestowing the award. "Their sterling achievements demonstrate how deep theoretical research drives practical applications in information and communication technology that shape our daily lives."

**Madrid, January 16, 2018.-** The BBVA Foundation Frontiers of Knowledge Award in the Information and Communication Technologies category goes, in this tenth edition, to Shafi Goldwasser, Silvio Micali, Ronald Rivest and Adi Shamir for their "fundamental contributions to modern cryptology, an area of a tremendous impact on our everyday life," in the words of the jury's citation. "Their advanced crypto-protocols enable the safe and secure transmission of electronic data, ranging from e-mail to financial transactions. In addition, their work provides the underpinning for digital signatures, blockchains and crypto-currencies," like Bitcoin.

The work of Goldwasser, Micali, Rivest and Shamir, the citation adds, "is crucial to the fabric of our connected digital society. Every time we log in to social media, purchase goods online, or vote or sign electronically, we leverage the technology developed by their research."

For the jury, the rise of today's digital age could never have happened without techniques that ensure the secure exchange, use and storage of information. Cryptography is an "invisible" technology that is nonetheless indispensable for today's society. Over the space of four decades, the new laureates have not only laid the foundations of this complex field, but have also continued to enlarge it with breakthroughs that exploit the possibilities of the vast wealth of information now at our command, the famous Big Data, or have driven the development of potentially world-changing technologies like crypto-currencies.

"Human societies have always needed secure communication," the jury remarks, and this need has become increasingly acute. The design of openly available communication protocols accordingly represents "a great research challenge, which was tackled superbly by the awardees."

In 1978, Adi Shamir and Ronald Rivest, together with Leonard Adleman, created the RSA algorithm (whose initials correspond to their surnames). The "first of the secure protocols that defined the face of modern cryptography," as the jury terms it, RSA is what is known as a "public-key" encryption system, because each user has two keys: a public key, used to encrypt the message; and another one known only to the receiver. The encryption process is based on a mathematical problem intractable for today's computers – in this case the factoring of a multi-digit number – without the aid of the other, private key. RSA is still a widely used protocol, particularly in combination with other techniques.

Shamir and Rivest, now working respectively out of Israel's Weizmann Institute and the Massachusetts Institute of Technology (USA), arrived at this first breakthrough while collaborating closely at MIT, and in the forty years since then have continued to contribute actively in diverse areas of cryptography.

Goldwasser was then studying at Carnegie Mellon University (USA) and Micali at the Sapienza University of Rome. A few years later, in 1982, the two coincided on a doctorate course at the University of California, Berkeley (USA) and embarked on a fruitful collaboration whose first big result would lay the theoretical foundations of the field – the mathematical demonstration of when an encryption method is genuinely unbreakable.

As Micali explained in a phone conversation last night, "for thousands of years people have been trying to encrypt messages, but these were only secure until the moment they stopped being so, because someone had unlocked the code. RSA proposed an encryption scheme that no one could to break, but at the same time no one could prove was unbreakable. To prove a thing is secure, you need to go further. You want to be sure that no future attack can succeed. Our contribution was to apply a rigorous method to ensure that if someone wants to understand part of an encrypted message, they would first have to solve a mathematical problem that has stood unsolved for hundreds of years."

Following on from these seminal achievements, Goldwasser and Micali, together and separately, "have expanded the scope of cryptography beyond its

traditional goal of secure communication," in the view of the jury, with developments that have helped build today's flourishing digital society by allowing users to collaborate, share information and shop online without sacrificing security.

For instance, both scientists contributed (with Charles Rackoff) to the development of the "zero-knowledge proof," which shows that it is possible to convince your interlocutor of the truth of something without revealing what that something is. The result is an algorithm that underlies a wide range of applications from authentication processes to Bitcoin transactions. Talking last night after hearing the award, the two laureates offered as examples logging in to a social network with your password, ordering transactions in your online bank account, or making payments with crypto-currencies.

"In our daily lives, any 'password' we type or digital signature we use is protected by techniques based on our work," says Micali.

Goldwasser, meantime, singled out another contribution, vital to properly harness the power of big data. When a series of organizations pool their databases to extract the greatest possible amount of information from the resulting aggregate, but without disclosing the identity embedded in the data.

She believes it is vital that citizens learn to value their personal data, and stop giving them away for free, insisting that, with today's cryptographic tools, privacy and security are readily compatible. She is also convinced of the area's huge untapped potential: "We have effective cryptographic methods that are still not being used… IT firms should do more to build systems to make use of the beautiful ideas we have come up with in the cryptographic field that have never been implemented."

Rivest and Shamir too have continued to contribute valuable ideas and solutions. Rivest, specifically, created a popular algorithm with the ability to check that a given file – downloaded from the internet, for instance – has not been tampered with. Shamir, meantime, has developed the area of differential cryptanalysis, a method for decrypting secret keys.

On being informed of the award, Rivest remarked on how much cryptography, and society with it, has changed during his career: "In the late 1970s, we didn't even have the World Wide Web, it was impossible to imagine that our method would become what it is today... Right now, each time we make an online purchase, the transaction's security is based on our encryption technology, and it is thanks to this technology that we can be sure we are talking to Amazon, and vice versa."

The bitcoin and blockchain technologies are another topic currently occupying these four experts. For Rivest, "Bitcoin is an interesting technology, but the truth is there is a lot of hype associated with the phenomenon and it is too early to say whether it will become a reliable system capable of ushering in the new digital economy."

## Laureate bio notes

### Shafi Goldwasser

Shafrira Goldwasser (New York, USA, 1958) graduated in mathematics from Carnegie Mellon University, then went on to earn a PhD in Computer Science from the University of California, with a thesis on the theory and practice of probabilistic encryption. In 1983, she joined the Massachusetts Institute of Technology and by 1995 was a full professor, as well as co-leader with Ronald Rivest of the Cryptography and Information Security Group. Since 1997, she has held the RSA Professorship of Electrical Engineering and Computer Science, established that same year under an agreement with RSA Data Security, the firm set up by Ron Rivest, Adi Shamir and Leonard Adelman after developing the algorithm to which they lent their names.

She is also a member of the Theory of Computation Group and co-leads the Cryptography Group in the MIT Computer Science and Artificial Intelligence Laboratory. Since 1993, she has combined these responsibilities with the post of Professor of Computer Science and Applied Mathematics at the Weizmann Institute of Science (Israel), where she is a member of the Theory Group.

### Silvio Micali

Silvio Micali (Palermo, Italy, 1954) graduated in mathematics from Sapienza University of Rome and earned a PhD degree in Computer Science from the University of California, Berkeley. In 1983 he joined MIT, where he is currently a full professor and associate head of the Department of Electrical Engineering and Computer Science. Like Rivest and Goldwasser, he works in the MIT Computer Science and Artificial Intelligence Laboratory.

His research focuses on information security. He has worked, like Adi Shamir, on the zero-knowledge proof and has been distinguished jointly with Shafi Goldwasser for his cryptographic research. Author of *Randomness and Computation* (from the series "Advances in Computing Research"), he has 47 patents to his name and is the founder of two companies: CoreStreet, providing smart credential software – acquired by ActiveIdentity in 2009 – and Peppercoin, which he set up with Ronald Rivest to market a cryptographic system for processing micropayments.

### Ronald Rivest

Ronald Rivest (Schenectady, USA, 1947) holds a bachelor's degree in Mathematics from Yale University and a PhD in Computer Science from Stanford University. In 1974 he joined the Massachusetts Institute of Technology, where he is currently Institute Professor – the highest academic rank, held by fourteen of MIT's over one thousand faculty members – in the Department of Electrical Engineering and Computer Science.

Rivest is founder and currently co-leader with Shafi Goldwasser of the Cryptography and Information Security Group in the MIT Computer Science and Artificial Intelligence Laboratory. He is co-author of *Introduction to Algorithms*, a standard textbook in the subject area, and a past director of both the International Association for Cryptologic Research and the Financial Cryptography Association. He has founded three companies: RSA Data Security, Verisign – which came to be Internet's leading encryption, certification and authentication authority – and Peppercoin, in partnership with Silvio Micali.

### Adi Shamir

Adi Shamir (Tel Aviv, Israel, 1952) received a BSc in Mathematics from Tel Aviv University and went on to obtain a PhD in Computer Science in 1977 from the Weizmann Institute of Science. From 1977 to 1983, he was a researcher and assistant professor at MIT. It was there he met Ron Rivest and Len Adleman, with whom he went on to invent the RSA algorithm. After completing his stay at MIT, he returned to the Weizmann Institute, where he now holds the Borman Professional Chair of Computer Science.

As well as his work on RSA, secret sharing and differential cryptanalysis, the Israeli scientist succeeded in breaking the Merkle-Hellman cryptosystem, one of the first public-key schemes in existence. He is also the designer of the TWIRL and TWINKLE factoring devices, the author of identify-based cryptography and inventor of visual cryptography, based on breaking up an image – which could be a text – such that the resulting pieces appear to be a random scattering of black and white pixels.

### ICT jury and technical committee

The rigor, quality and independence of the judging process has earned these awards the attention of the international scientific community and a firm place among the world's foremost prize families.

The jury in this category was chaired by **Georg Gottlob**, Professor of Informatics at the University of Oxford (United Kingdom) and Adjunct Professor of Computer Science at Vienna University of Technology (Austria). The secretary was **Mario Piattini**, Professor of Computer Languages and Systems and head of the Alarcos Research Group at the University of Castilla-La Mancha (Spain). Remaining members were **Regina Barzilay**, Delta Electronics Professor un the Department of Electrical Engineering and Computer Science at Massachusetts Institute of Technology (USA), **Liz Burd**, Pro-Vice Chancellor in Learning and Teaching at the University of Newcastle (Australia)**, Ron Ho,** Senior Director of Engineering in the Programmable Solutions Group at Intel Corporation (USA), **Rudolf Kruse**, Emeritus Professor of Computer Science at the University of Magdeburg (Germany), and **Joos Vandewalle**, president of the Royal Flemish Academy of Sciences and Arts of Belgium and Emeritus Professor in the Department of Electrical Engineering (ESAT) at Katholieke Universiteit Leuven (Belgium).

The **CSIC Technical Committee** was coordinated by **María Victoria Moreno**, the Council's Deputy Vice President for Scientific and Technical Areas, and formed by: **Carmen García**, Coordinator of the Physical Science and Technologies Area and Research Professor in the Institute of Corpuscular Physics (IFIC); **Roberta Zambrini**, Tenured Researcher in the Institute of Interdisciplinary Physics and Complex Systems (IFISC); **Federico Thomas,** Research Professor in the Institute of Robotics and Industrial Computing (IRII); **Juan Antonio Rodriguez,** Tenured Researcher in the Institute of Research in Artificial Intelligence (IIIA); and **Ángela Ribeiro**, Tenured Researcher in the Center for Automation and Robotics (CAR); and.

## About the BBVA Foundation Frontiers of Knowledge Awards

The promotion of knowledge based on research and artistic and cultural creation, and the interaction of these domains, forms a core strand of **the BBVA Foundation**'s action program, along with the recognition of talent and excellence across a broad spectrum of disciplines, from science to the arts and humanities.

In line with these objectives, the **BBVA Foundation Frontiers of Knowledge Awards** were established in 2008 to recognize outstanding contributions in a range of scientific, technological and artistic areas, together with knowledge-based responses to the central challenges of our times. The areas covered by the Frontiers Awards are congruent with the knowledge map of the 21st century, in terms of the disciplines they address and their assertion of the value of cross-disciplinary interaction.

Their **eight categories** span classical areas like Basic Sciences (Physics, Chemistry and Mathematics), Biomedicine and other areas characteristic of our time, like Biomedicine, Information and Communication Technologies, Ecology and Conservation Biology, Climate Change, Economics, Finance and Management and Development Cooperation, and the particularly innovative realm that is Contemporary Music.

The BBVA Foundation is aided in the evaluation process by the **Spanish National Research Council (CSIC)**, the country's premier public research organization. As well as designating each jury chair, the CSIC is responsible for appointing the technical evaluation committees that undertake an initial assessment of candidates put forward by numerous institutions across the world and draw up a reasoned shortlist for the consideration of the juries.

## CALENDAR OF UPCOMING AWARD ANNOUNCEMENTS

| | |
|---|---|
| **Basic Sciences** | Tuesday, January 23, 2018 |
| **Biomedicine** | Tuesday, January 30, 2018 |
| **Ecology and Conservation Biology** | Tuesday, February 6, 2018 |

| | |
|---|---|
| **Contemporary Music** | Tuesday, February 13, 2018 |
| **Economics, Finance and Management** | Tuesday, February 20, 2018 |
| **Development Cooperation** | Tuesday, February 27, 2018 |

**LAUREATE'S FIRST DECLARATIONS AND IMAGES**

A video recording of the new laureate's first interview on receiving news of the award is available from the Atlas FTP with the following coordinates:

Server: **5.40.40.61**

Username: **AgenciaAtlas4**

Password: **mediaset17**

The name of the video is:

**"PREMIO TIC"**

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

**Mobile:** +34 619 30 87 74

**E-mail:** mgil@mediaset.es

Fundación BBVA

For more information, contact the BBVA Foundation Department of Communication and Institutional Relations (+34 91 374 5210; 91 374 3139; 91 374 8173/ comunicacion@fbbva.es) or visit www.fbbva.es