THE JAPAN PRIZE FOUNDATION

ARK Mori Building, East Wing 35th Floor, 1-12-32 Akasaka, Minato-ku, Tokyo, 107-6035, JAPAN Tel: +81-3-5545-0551 Fax: +81-3-5545-0554 www.japanprize.jp



Japan Prize News No. 57 Feb. 2017

JAPAN PRIZE

2017 Japan Prize Laureates Announced

This year's Japan Prize will be awarded to Dr. Adi Shamir, for his significant contributions to information security through his pioneering research on cryptography, and jointly to Prof. Emmanuelle Charpentier and Dr. Jennifer A. Doudna for the development of a revolutionary new technology in genetic engineering.

"Electronics, Information and Communication" field

"Life Science" field



Dr. Adi Shamir Professor, Weizmann Institute of Science

Israel





ance



Dr. Jennifer A. Doudna Professor, University of California, Berkeley

United States

The Japan Prize Foundation has decided to award the 2017 (33rd) Japan Prize to Dr. Adi Shamir of Israel, Prof. Emmanuelle Charpentier of France and Dr. Jennifer A. Doudna of the United States.

In the field of "Electronics, Information and Communication," Dr. Adi Shamir is being honored for "contributions to information security through pioneering research on cryptography."

Dr. Shamir's achievements span from the development of the "RSA cryptosystem," an innovative encryption technique utilizing mathematical methodology, to the proposal of the "secret sharing scheme" which ensures secrecy by breaking up classified information into parts and dispersing it among several participants, the "identification scheme" through which individuals can be identified without revealing secret information, and the generic "differential cryptanalysis" which deciphers common key cryptosystems.

These remarkable achievements have transformed cryptography from a mere technology to the academic discipline of "cryptology." Furthermore, by developing cryptosystems which form the basis of information security, Dr. Shamir has paved the way to the fast and convenient open digital network environment that we take for granted today.

Prof. Emmanuelle Charpentier and Dr. Jennifer A. Doudna are being honored for their remarkable achievement in the field of "Life Science" through the "elucidation of the genome editing mechanism by the CRISPR-Cas."

Genome editing using the CRISPR-Cas system, developed by Prof. Charpentier and Dr. Doudna, is truly a revolutionary technique in genetic engineering that is far more economical and speedy than those previously available. This overwhelmingly simple technique enables one to cut the DNA of any organism at arbitrary locations to edit freely by means of removing, replacing or insertion. It was adopted at an explosive pace as a research tool in the life sciences, and is now being applied to research in a wide range of fields, such as breeding, drug development and medicine.

As described, the achievements of the three laureates are deemed most eminently deserving of the Japan Prize given to honor contributions to the advancement of science and technology which further the cause of peace and prosperity of mankind. The award presentation ceremony to honor the laureates will be held on April 19 of this year at the National Theatre in Tokyo.

JAPAN PRIZE

The Japan Prize came into being after the late Mr. Konosuke Matsushita, the founder of Matsushita Electric Industrial Co., Ltd. (now known as Panasonic Corporation), responded in 1982 with a personal donation to the then government's wish to create a prestigious international prize for scientists from around the world as a token of gratitude to international society. With a cabinet endorsement, the Prize was first awarded in 1985. Since that year, the Japan Prize Foundation has awarded the Japan Prize to 88 laureates from 13 countries, to date.

"Electronics, Information and Communication" field

Achievement : Contribution to information security through pioneering research on cryptography

Dr. Adi Shamir (Israel)

Born: July 6, 1952 (Age: 64, Nationality: Israel) Professor, Weizmann Institute of Science

Summary

The advent of open digital networks, namely the Internet, has enabled us to lead a convenient lifestyle like never before. Such comfort has been made possible thanks to security measures preventing the theft and manipulation of valuable information. It is Dr. Adi Shamir who proposed many of the underlying concepts in information security and developed a series of practical solutions.

Information in digital networks is coded in binary digits. Utilizing mathematical methodology, Dr. Shamir has invented and proposed numerous techniques, such as the innovative "RSA cryptosystem," the "secret sharing scheme" which ensures secrecy by breaking up classified information into parts and dispersing it among several participants, the "identification scheme" with which individuals can be identified without revealing secret information and the generic "differential cryptanalysis" which deciphers many common key cryptosystems.

Dr. Shamir has also made a significant breakthrough in the research of side-channel attacks which decipher code by monitoring the physical information of the computer carrying out encryption, such as power consumption and noise.

Co-developing the first practical public-key cryptography with two MIT researchers

Cryptography plays an important role in our lives, but for a long time, it was primarily used by specific groups in society such as the government and the military. In such cases, the same cryptographic key was used for both encryption and decryption, and was secretly shared among specific individuals in the group. However, as open digital networks emerged and a large number of unspecified users began to exchange information, the need for a new cryptosystem arose to overcome major issues of safety surrounding the distribution and sharing of cryptographic keys.

In 1976, Stanford University researchers Dr. Whitfield Diffie and Dr. Martin Hellman proposed a new cryptosystem called the "public key cryptography." The system has two types of keys, the encryption key which is open to the public, and the decryption key which is kept private. This scheme allows a large number of unspecified people to send secret information encrypted with a public key, which can only be decrypted by the intended recipient. This enables secure transactions, such as shopping over the internet with a credit card.

Its first practical realization, the "RSA cryptosystem," was co-developed in 1977 by three young researchers at MIT (Massachusetts Institute of Technology), namely Dr. Ron Rivest, Dr. Adi Shamir, and Dr. Leonard Adleman.

Intrigued by the proposal of public key cryptography, Dr. Rivest and Dr. Shamir explored encryption methods using various mathematical techniques. Joining midway through the research, Dr. Adleman searched for flaws that could lead to decryption. After numerous trials, they finally succeeded with their 43rd iteration, and named it the RSA cryptosystem taking the first letter of the three doctors' names.

The essential basis of this cryptosystem lies in the difficulty in the prime factorization of very large numbers (the product of two prime numbers). The product of two prime numbers is publicly released as the encryption key. In order to uncover the decryption key, one needs to perform prime factorization on the encryption key, and identify the two prime numbers. The product of two prime numbers used in today's RSA cryptosystem expressed in binary is between 2²⁰⁴⁸ and 2⁴⁰⁹⁶, much greater than the total number of atoms in a galaxy, which is 2²²³. Even a supercomputer would be unable to compute this in 10 thousand years.

The RSA cryptosystem can also be used as a signature mechanism. A message encrypted using the decryption key can in turn be decrypted using the encryption key, allowing anyone to verify the signatory as the one with the decryption key.

The invention of the secret sharing scheme which protects information from disasters

Information dispersal is crucial for the secure storage of important data. In 1979, Dr. Shamir was the first to propose the "secret sharing scheme," which specifies the dispersal method that ensures the security of information depending on the extent of dispersed information leakage. This was achieved using the polynomial method.

Based on the fact that a straight line is a first degree polynomial, and a parabola is a second degree polynomial, secret information is represented as points on the polynomial. Points other than the secret information are dispersed and stored. By doing so, a first degree polynomial requires two pieces of dispersed information. and that of the second degree requires three pieces of dispersed information to recover the secret information. This is because two points are sufficient to draw a straight line with accuracy, and three points for a parabola. Similarly, for a polynomial of order k, the secret information can be recovered by gathering k+1 pieces of dispersed information. By dispersing information into k+1 pieces or more, up to k pieces of information can be stolen without it being disclosed, and even if several of them are damaged, it can be restored as long as k+1 pieces remain safe. By using this scheme, valuable data can be dispersed according to its intended purpose. As an earthquake countermeasure, for example, information can be dispersed across three separate locations around the country. Even if information in one of the locations is destroyed in an earthquake, data can be recovered using information from the other two locations.

In addition, Dr. Shamir invented the "visual secret sharing scheme." It involves splitting an image into two or more sandstorm-like patterns, which, when overlapped, reveal the original image. The separated images are expressed as light and dark dots that, when overlapped, manifests as light-light, light-dark or dark-dark overlay, thereby reproducing the original image.

Following Dr. Shamir's proposal of the "secret sharing scheme," a diverse range of variants has been studied by numerous researchers. Besides being adopted for practical use, this scheme has also been applied to other cryptographic technology, thereby contributing enormously to the advancement of cryptographic technology research.

An identification scheme that does not reveal any secret information

In the physical world, IDs such as a driver license must be presented in order to prove one's identity. In digital networks, however, presenting secret information such as a password poses a risk of it being stolen, which could lead to identity theft.

In 1986, Dr. Shamir developed an "identification scheme," which proves one's possession of authentic secret information during a transaction without revealing any of it to the other party. Based on the mathematical theory of quadratic residue, it is a magnificent achievement both academically and practically, and has been adopted by satellite broadcasting services in billing systems that guarantee the authenticity of its users.

The discovery of a generic method for decrypting common-key cryptosystems

Advancement in cryptographic technology requires not only the development of new technology but also the discovery of flaws in existing technology. The RSA cryptosystem by Dr. Shamir's group was developed to hold up against Dr. Adleman's deciphering tests. Dr. Shamir himself studied the risk of illegitimate deciphering in great depth and has made important suggestions on the topic.

In 1990, Dr. Shamir demonstrated that many common key cryptosystems could be deciphered, by analyzing the statistical differences in the differential values of two encrypted messages which results in parts of

JAPAN PRIZE



the encryption process canceling each other out.

Many common key cryptosystems encrypt information by the repeated application of simple encryption process, and are therefore prone to such a decryption method. Dr. Shamir went on to prove that it is possible to decipher the DES (Data Encryption Standard), adopted by the National Bureau of Standards (NBS, today's NIST) in 1977 as the world's first encryption standard for commercial transaction, if only eight or so iterations of the encryption processes are performed.

In practice, DES was never cracked as it had been encrypting information 16 times over. This discovery, however, spurred the development of a safer cryptosystem and led to NIST's adoption of a new encryption standard in 2000.

Deciphering encryption using a smartphone placed beside a PC

Deciphering information by analyzing the activities of the encryption and decryption program based on fluctuations in the computer's physical information, such as power consumption and machine noise, is called a side-channel attack. From an early stage, Dr. Shamir focused on side-channel attacks and made numerous breakthroughs.

In 2014, Dr. Shamir demonstrated that it is possible to break the RSA encryption, developed by him and his colleagues, by analyzing the machine noise picked up by a smartphone placed beside the computer. Such findings hold important significance for the future design of secure systems including the hardware.

As described, Dr. Shamir, through 40 years of research, has transformed cryptography from a minor technology for the few to the academic discipline of "cryptology."

In an era in which the rise of open digital networks has enabled the people of the world to freely exchange information, Dr. Shamir has consistently pioneered the frontiers of information security research and created new research trends. With the emergence of intelligent computing such as A.I., great anticipation is building around the future of Dr. Shamir's research.

"Life Science" field

Achievement : Elucidation of the genome editing mechanism by the CRISPR-Cas

Prof. Emmanuelle Charpentier (France) Born: December 11, 1968 (Age 48) Director, Max Planck Institute for Infection Biology (Berlin)

Dr. Jennifer A. Doudna (USA)

Born: February 19, 1964 (Age 52) Professor, University of California, Berkeley

Summary

Genome editing using the CRISPR-Cas system, announced by Prof. Emmanuelle Charpentier and Dr. Jennifer Doudna in 2012, is a revolutionary new technology in genetic engineering. It was adopted at an explosive rate as a useful tool for research in the life sciences. Today, it continues to be applied to research in a wide range of fields, such as breeding, drug development and medicine. This technology was developed in the process of elucidating the bacterial defense mechanism against such threats as viral infections. Bacteria can remember the DNA of intruding viruses by absorbing their DNA into their own. Upon the next infection, bacteria recognize the intruder's DNA and snips it with the RNA-guided CAS protein, thereby destroying intruding viruses. Genome editing by the CRISPR-Cas system takes advantage of this mechanism, and enables one to cut the DNA of any organism at arbitrary locations to edit freely by means of removing, replacing or insertion.

Meeting of two female scientists results in a long distance research collaboration

CRISPR is an abbreviation for Clustered Regularly Interspaced Short Palindromic Repeats. Bacteria genomes frequently contain repeating structures of palindrome-like identical sequences, made up of 20 to 50 bases, in between short sequences (spacers).

This repeating structure is CRISPR. It is sometimes called the CRISPR locus including the genes that code the string of adjoining Cas (CRISPR associated) proteins.

This repeating sequence came to be recognized as genome sequencing of many bacteria and archaebacteria advanced, but its role was initially a mystery. Later on, it was discovered that spacer sequences are not inherent in bacteria, but are derived from foreign viruses and plasmids. It was then hypothesized that CRISPR's role is to provide bacteria with adaptive immunity against intruders, which was later proven to be the case.

The fact that small unicellular bacteria possess an ingenious immune system was received with great surprise and spurred research on how bacteria fight off invaders. This is the mechanism that was elucidated by Prof. Charpentier and Dr. Doudna. The two met in Puerto Rico in March 2011 at the conference on "Regulating with RNA in Bacteria" hosted by the American Society for Microbiology, and began their joint research immediately thereafter.

Prof. Charpentier, born in France, is a microbiologist with a PhD from Institut Pasteur. At the time, she was working at Umea University in Sweden, near the arctic region.

In the early 2000s, when she headed a small laboratory at the University of Vienna, she became interested in CRISPR, which had not yet received much attention. By 2009, she had discovered that two RNA and Cas9 protein in the streptococcus pyogenes genome play an important role in a bacterium's immune system.

Already at this point, Prof. Charpentier believed in its potential as a new technology for genetic engineering.

Dr. Doudna, on the other hand, graduated with a PhD from Harvard University where she studied RNA enzymes (ribozymes). As a structural biologist, she has since consistently researched the various functions of RNA, including the elucidation of the three-dimensional structure of ribozyme crystals.

From 2002, she has worked as a professor at the University of California, Berkeley. Since she became aware of the hypothesis about CRISPR's potential role in the adaptive immunity of bacteria around 2005, she had been conducting research to elucidate the role of RNA in the defense mechanism of cells.

Looking back, Dr. Doudna feels that upon meeting Prof. Charpentier, intuition told her they could complement each other through joint research. Thus began a long distance research collaboration bridging Northern Europe and the West Coast of the United States, which soon produced results that would astonish the world.

The birth of a genome editing technology that enables us to freely rewrite DNA

Already in June of the year following their first meeting, the joint research group used the DNA of streptococcus pyogenes provided by Prof. Charpentier to elucidate the detailed mechanism of how the two RNA and the bacteria's Cas protein (Cas9) cut foreign DNA. Along with the discovery, they also demonstrated that this knowledge can be converted into a revolutionary genome editing technology. It was an achievement that truly took the world by storm.

When a bacterium is invaded by a foreign virus, the invader's DNA is fragmented by the Cas enzyme and stored in the CRISPR locus as spacer sequences. If the bacterium detects the same invader again, short-chain CRISPR RNA (crRNA) is produced using the stored spacers as the template.

crRNA then forms a compound with trans-activating crRNA (tracrRNA) which provides the base for the Cas protein. This compound (gRNA) guides the Cas enzyme to its complementary location in the invader's DNA.

The Cas9 enzyme that snips the DNA strand has two DNA incision sections, with one section cutting one of the strand and the other section cutting the opposite strand. The markers used for incision are short sequences approximately three-base-long called PAM (Pro-to-spacer Adjacent Motif) located throughout the intruder's DNA. The Cas9 enzyme coming in contact with PAM triggers incision.

Having elucidated this mechanism, their research group demonstrated that by designing and synthesizing gRNA that corresponds to the target DNA locus, and introducing it into a cell together with Cas9, the target DNA can be discriminately cut at as many PAM positions as desired with pinpoint accuracy.

The incision site of target DNA is recombined by an intracellular repair mechanism, but due to the shift that occurs in the base sequence, the gene loses its function and becomes knocked out. Furthermore, introducing a base sequence into the incision site induces homologous recombination repair, resulting in the insertion of this base sequence into the DNA.

It is without a doubt that the whole world was excited by the discovery of a new genome editing technology that is highly versatile, precise and efficient. Thanks to its low cost and speediness compared to existing techniques such as ZFN and TALEN, as well as its overwhelming simplicity, CRISPR has attracted many researchers and spurred further trial and research.

25 years since the discovery of a mysterious sequence – The future of genome editing

The mysterious repeating sequence in the DNA of bacteria was first observed back in 1987. Dr. Yoshizumi Ishino of the Research Institute for Microbial Diseases at Osaka University reported the existence of a mysterious base sequence in E. coli, concluding his report with the words, "its biological significance is unknown".

25 years on, this mysterious base sequence has been adapted

JAPAN PRIZE



into the CRISPR-Cas9 technology which enables us to edit the genome of all living things, and is on the verge of bringing about unprecedented technological innovation across various disciplines of the life sciences.

The development and improvement of the CRISPR-Cas9 technology has since become very competitive, with researchers striving to improve precision and ease of use.

Its popularity has been so remarkable that tailored kits have now become available, and there is even a commercial genome editing service operating with success.

In early 2013, the first genome editing of a mammalian cell using CRISPR-Cas9 was performed. Today, genome editing of human cells, such as those in conjunction with iPS cells, has advanced to the stage where it is now aiming for clinical application. The fields of agriculture and livestock breeding are also seeing much activity with promising research efforts.

While genome editing technology has the potential to revolutionize the future of mankind, there are also growing concerns over the ethical issues it raises and its negative impact on the ecosystem, as exemplified by the genetic modification of reproductive cells and the eradication of specific organisms.

From early on, Dr. Doudna has been a vocal advocate on these issues and proposed discussion amongst the scientific community. At the 2015 "International Summit on Human Gene Editing" hosted by the National Academy of Sciences of the United States, a consensus for a certain level of restraint on human gene editing research was reached. Cautiously yet resolutely, scientists' efforts in genome editing are rapidly transforming the field of life science within just a few years from the innovative breakthrough achieved by Prof. Charpentier and Dr. Doudna's joint research.

After the remarkable achievement of their joint research, the two scientists are now pursuing new research in their respective fields. Prof. Charpentier is now the director of the Max Planck Institute for Infection Biology and has also founded a venture business on gene therapy. Similarly, Dr. Doudna has founded a venture business and is collaborating with biotech companies to apply her technology into a wide range of fields.

There is great anticipation in the future activity of Prof. Charpentier and Dr. Doudna.

Nomination and Selection Process

- Every November, the Field Selection Committee of The Japan Prize Foundation designates and announces two fields in which the Japan Prize will be awarded two years hence. At the same time, the Foundation calls for over 13,000 nominators, strictly comprised of prominent scientists and researchers from around the world invited by the Foundation, to nominate the candidates through the web by JPNS (Japan Prize Nomination System). The deadline for nominations is the end of February of the following year.
- For each field, a Selection Subcommittee conducts a rigorous evaluation of the candidates' academic achievements. The conclusions are then forwarded to the Selection Committee, which conducts evaluations of candidates' achievements from a wider perspective, including contributions to the progress of science and technology, and significant advancement towards the cause of world peace and prosperity, and finally the selected candidates are recommended for the Prize.
- The recommendations are then sent to the Foundation's Board of Directors, which makes the final decision on the winners.
- The nomination and selection process takes almost one year from the time that the fields are decided. Every January, the winners of that year's Japan Prize are announced. The Presentation Ceremony is held in April in Tokyo.



Members of the 2017 Japan Prize Selection Committee



(alphabetical order, titles as of December, 2016)

Fields Eligible for the 2018 Japan Prize

Area of Physics, Chemistry and Engineering
Resources, Energy, Environment and Social Infrastructure

Background and rationale:

A major goal for humankind is the realization of the sustainable development of our society while overcoming various limitations in resources, energy, and the environment, as affirmed by the United Nations' Sustainable Development Goals (SDGs) in 2015. Widening social disparity and the increasing number of communities vulnerable to disasters are of growing concern, as the impact of climate change accumulates and urbanization intensifies.

Thus, we are in serious need of further innovation in the effective development, utilization and recycling of water and resources, various energy-related technologies, and social infrastructure technologies for cities and transportation systems. Another key challenge is to spur innovation in fundamental technologies for the realization of a resilient society capable of predicting and responding to environmental changes, as well as of preventing and mitigating natural and human made disasters.

Achievement eligible:

The 2018 Japan Prize in the field of "Resources, Energy, Environment and Social Infrastructure" is awarded to an individual(s) who has achieved breakthroughs in the creation, innovation, development or dissemination of science and technology, thereby contributing towards the sustainability of human society and the improvement of the global environment.

Life Science, Agriculture and Medicine Medical Science and Medicinal Science

Background and rationale:

In recent years, developments in modern science have brought about remarkable advancements in the field of medical science and medicinal science. Revolutionary medical technologies like individually optimized precision medicine driven by personalized diagnosis and genomic medicine, and regenerative medicine have been established one after another, alongside the elucidation of pathological mechanisms for various diseases. While diseases associated with aging and changes in lifestyle are on the rise, emerging infectious diseases and resistant bacteria, fueled by globalization, have also become a worldwide issue.

In such times of change, it is highly anticipated that medical science and medicinal science, integrated with other disciplines like engineering and information science, will make a greater contribution towards healthy living. These include the creation and spread of new medical treatments, the development and production of new drugs as well as the development of drug delivery systems.

Achievement eligible:

The 2018 Japan Prize in the field of "Medical Science and Medicinal Science" is awarded to an individual(s) who has achieved scientific and technological breakthroughs, such as new discoveries or the development of innovative technologies on the "prevention", "diagnosis", "treatment" or "prognosis" of diseases, thereby contributing towards the health and well-being of mankind.

Fields Selection Committee for the 2018 Japan Prize



(alphabetical order, titles as of December, 2016)

Schedule (2018-2020)

The fields eligible for the Japan Prize (2018 to 2020) have been decided for the two research areas, respectively. These fields rotate every year in a three year cycle.

Every year the Fields Selection Committee announces the eligible field for the next three years.

Area of Physics, Chemistry and Engineering		Area of Life Science, Agriculture and Medicine	
Year	Eligible Fields	Year	Eligible Fields
2018	Resources, Energy, Environment and Social Infrastructure	2018	Medical Science, Medicinal Science
2019	Materials, Production	2019	Biological Production, Biological Environment
2020	Electronics, Information and Communication	2020	Life Science