ISSN 0915-3160

平成三十一年一月十日発行（年四回一、四、七、十月の十日発行）通巻百二十一号 New Breeze

New Breeze

Quarterly of The ITU Association of Japan

No. 1
Vol. 31 January 2019
Winter

New Year Messages

From the Minister of Internal Affairs and Communications, Secretary-General of ITU, President of ITU-AJ

Special Feature

Trends in Quantum-related Technologies

R&D Trends and Future Prospects of Quantum Cryptography

Trends in Post-Quantum Cryptography: Cryptosystems for the Quantum Computing Era

Initiatives for New Computers using Quantum Technology

Development of a Combinatorial Optimization Calculation Engine

Overview of CMOS Annealing Machines

New Breeze ISSN 0915-3160
Quarterly of The ITU Association of Japan
BN Gyoen Bldg., 1-17-11 Shinjuku, Shinjuku-ku,
Tokyo 160-0022 Japan
Tel: +81-3-5357-7610 Fax: +81-3-3356-8170
https://www.ituaj.jp/?page_id=310

Letters to *New Breeze*

New Breeze welcomes readers' opinions. Please send comments with your name, address, and nationality by e-mail, fax, or post to the editor.

e-mail address: kikanshi@ituaj.jp

Subscription forms are available on the ITU-AJ website:
http://www.ituaj.jp/english/subscription_form.pdf

Subscription Fee:

Single issue:	¥1,500
Annual subscription (4 issues):	¥6,000

Disclaimer: Opinions expressed in this publication are those of The authors and do not necessarily represent those of The ITU Association of Japan.

CONTENTS

About ITU-AJ

The ITU Association of Japan (ITU-AJ) was founded on September 1, 1971, to coordinate Japanese activities in the telecommunication and broadcasting sectors with international activities. Today, the principle activities of the ITU-AJ are to cooperate in various activities of international organizations such as the ITU and to disseminate information about them. The Association also aims to help developing countries by supporting technical assistance, as well as by taking part in general international cooperation, mainly through the Asia-Pacific Telecommunity (APT), so as to contribute to the advance of the telecommunications and broadcasting throughout the world.

Greetings for the New Year 2019 from the Minister of Internal Affairs and Communications

Masatoshi Ishida
Minister of Internal Affairs and Communications

I wish you a Happy New Year.

In October last year, I had the honor of being appointed the Minister of Internal Affairs and Communications, and Minister of State for the Social Security and Tax Number System. The responsibilities of these positions are wide ranging, with many issues that relate closely to daily life, but I will work earnestly to meet the expectations of all citizens of Japan.

Enhancing ICT Infrastructure

Technologies like fifth-generation mobile communication systems (5G) and optical fiber are essential infrastructure for Society 5.0 and are the key to eliminating information disparity between urban and rural areas. We are working on the allocation of radio frequencies to expand 5G to all regions of Japan within two years, and preparing the budget to develop optical fiber infrastructure in all regions to make it available to all of Japan as quickly as possible. At the same time, we are revising the radio system to utilize radio frequencies more effectively, which includes a review of the frequency allocation system and fee structures.

Multi-lingual speech translation systems have already reached TOEIC 800 point levels for English, Chinese and Korean, so they are easy to use for daily conversation situations. We are continuing development and deployment so that it can be used with more languages and in more situations, to help in accepting foreign personnel, and in time for the Tokyo Olympic and Paralympic Games in 2020.

We also continue to promote R&D and standardization of advanced information and communications technologies, to strengthen use of IoT and AI in all industrial fields and to increase Japan's competitiveness in these industries. We are also actively working to introduce blockchain technologies, information trust functions, and a cashless economy, which are powerful forces for change in society.

As ICT continues to permeate our lives more broadly and deeply, society is increasingly vulnerable to threats such as cyber attacks. We are collaborating between government and private interests, on security measures for IoT and other devices that are potentially vulnerable, and at the same time, working to address social and consumer protection issues, toward a safe and secure ICT society.

Personnel development is also necessary for Society 5.0. We have multifaceted initiatives such as establishing "Community ICT Clubs" where children, students and others can learn programming and other skills, and regional human resource development to promote open data.

We are working to maximize utilization of ICT and realize a society in which each and every citizen can work and live in a manner that is suited to them, without being restricted by where they live, whether urban or rural. One initiative is "Telework Days", which promotes implementation of telecommuting on a national scale, providing flexibility to those that want to work and also helping to resolve overcentralized conditions in Tokyo. Another initiative promotes environments such as satellite offices and mobile work, which help people to work at times and places of their choosing, while living in the area they desire.

In December of last year, new 4K8K satellite broadcasts began, providing vivid, highly realistic viewing. We are using this 4K8K technology, together with communications technologies such as 5G, for tasks such as remote operation of machinery and remote medicine. Such use of advanced ICT will create environments that enable people to work and receive the services needed in their lives anywhere in Japan.

The benefits of Society 5.0 must be available to everyone, regardless of ability, age or geographical region. To achieve this, we are working on ICT to support it, including enhancements to captioning, descriptive, and sign-language broadcasts, to realize a society in which everyone can enjoy a wealthy life.

Developing ICT Internationally

This growth in Japan is inextricably linked to the international community. I will also be a co-chair of the G20 Ibaraki-Tsukuba Ministerial Meeting on Trade and Digital Economy next June. We will be promoting international cooperation on policy on important global issues in the future, such as development and utilization of AI and promoting free flow of information. As part of this, we are creating an ICT global strategy to unify ICT R&D and implementation in society, together with development overseas. This will advance development in Japan while also contributing internationally.

We are also actively working on expansion of infrastructure and systems overseas to maintain growth and capture markets there, utilizing our strengths in areas such as telecommunications, broadcasting, postal infrastructure, radio systems, statistics, disaster management, and administrative consultation systems. We are contributing to regional revitalization by expanding broadcast content overseas, increasing foreign tourism in disaster-affected and other areas, and expanding sales channels for regional products.

I would like to wish you all the best in the New Year, and I pray for the health and great happiness of all of you.

January 2019

Working together in 2019: New Year's message from the ITU Secretary-General

Houlin Zhao
Secretary-General
International Telecommunication Union

It is an honour for me to greet ITU's Japanese community via the ITU Association of Japan (ITU-AJ).

As a top ITU donor, a key contributor to ITU's technical work, and a global leader of connectivity initiatives for inclusive development, Japan is a particularly valued ITU partner.

Japan's industry, which includes many active, long-time Sector Members of ITU, has also been leading the way. In recent years, partnerships between the private sector and the Japan International Cooperation Agency have implemented innovative cooperative projects to use ICTs to drive development solutions in developing countries. For example, Fujitsu worked in Vietnam to use ICTs to improve the safety, productivity stable supply of agricultural products.

As countries use the power of ICTs to help accelerate progress towards the SDGs, I encourage them to follow Japan's example and focus their efforts on promoting infrastructure, investment, innovation and inclusivity.

Partnership is part of ITU's DNA. As the United Nations specialized agency for information and communication technology (ICT), ITU relies on the collaboration of 193 Member States and over 800 industry, academic and other members to manage spectrum and satellite orbits, develop relevant global standards on communication technologies and services, and assist developing countries for infrastructure and policy development on ICTs so they can accelerate progress towards the UN Sustainable Development Goals (SDGs). ITU's wide partnership is key to ensuring this work has global reach, relevance, and impact.

As 2018 draws to a close, I would like to reflect on a few of our collective achievements as a Union.

Together, we have made steady progress by leading the work on new innovations — bringing together stakeholders to ensure new technologies are green, efficient, secure, and cost-effective worldwide. And together, we have made important strides towards bridging digital divides so that everyone, everywhere, can benefit from the Internet and the vast resources it provides. So as we start to look forward to 2019 and beyond, I encourage our partners to continue working as team so that we can achieve success together.

Leading the work on new technologies

The world of technology is changing rapidly, and ITU is changing with it.

Now more than ever, ITU is working on how to provide better ICT services to the people and deliver on the promise of the Fourth Industrial Revolution.

Over the last few years, ITU has been at the forefront of this revolution. We have been working on issues ranging from artificial intelligence, smart cities, and digital currency to the Internet of Things, new television, and 5G standards. And we have facilitated ICT infrastructure development.

As we look forward to a new year, ITU's World Radiocommunication Conference 2019 (WRC-19) will further address these demands by considering new allocations and identifications for 5G systems, High Altitude Platforms, and non-geostationary satellites systems. Consensus is being built in its preparation to make it a new success for our Union.

Partnering for ICTs for development

Despite the progress, however, about half the world's population remains unconnected and unable to benefit fully from the digital revolution.

That's why ITU is increasing its role as a key partner in development.

To achieve the SDGs, we are supporting Member States and other stakeholders to make broadband Internet accessible, affordable, and relevant to everyone.

ITU has convened a wide range of stakeholders to enable global harmonized regulations and standards leading to economies of scale and interoperability, which have led to a continued decline in the prices of ICT services and devices. Nearly 4.4 billion active mobile broadband subscriptions are expected worldwide by end 2018.

In addition, we are increasing our collaboration with sister UN agencies and others on important common projects, leveraging the power of ICT to accelerate progress towards the SDGs.

In this effort, ITU has tackled issues ranging from digital literacy to health to financial inclusion. We can be proud of what we are doing with organizations like the Broadband Commission to promote infrastructure development, the International Labour Organization to train tomorrow's workforce, and UN Women to bridge the digital gender divide with initiatives such as EQUALS.

Building skills and creating opportunities for progress and prosperity

ITU is also leading the way to build ICT skills to help young people and others capitalize on the job opportunities of the digital era.

This year, ITU, UN Women, and the African Union launched a new initiative to equip girls and young women in Africa with digital literacy skills.

We also published ITU's Digital Skills Toolkit, which provides recommendations for government policymakers, as well for partners in the private sector, non-governmental organizations, and academia to contribute towards equipping millions young people with job-ready digital skills.

And ITU supported the success of young innovators at ITU Telecom World 2018, in Durban, South Africa. The event, which welcomed more than 3100 participants from 94 countries gave tech entrepreneurs the opportunity to meet investors, get advice from mentors, and gain visibility through ITU Telecom Awards.

Working together to achieve success

I feel very encouraged by our accomplishments and trust that, as long as we continue working together, we will succeed in making great strides towards sustainable and inclusive development.

Great things can happen when a wide variety of specialized groups and individuals are motivated to achieve a common set of goals. So I look forward to our continued work with ITU-AJ, Japan, and all of our ITU members, with a renewed focus on the 2030 development agenda.

I wish you all a peaceful, healthy, and happy 2019.

New Year Greeting

Toru Fukuoka
President
The ITU Association of Japan

2019 promises to be an exciting year. We are finally entering the era of IoT, where everything is connected to the network. Not only that, we expect to see the emergence of advanced and highly accurate services based on AI technology.

Ordinary households are already starting to use smart speakers that employ AI technology for purposes such as gathering information and controlling domestic appliances. Significant advances are also being made in the technology used to control robots and operate self-driving vehicles and drones. At the end of last year, we saw the introduction of 4K/8K satellite broadcasting, and the launch of Japan's independent global positioning service based on the four *Michibiki* satellites. Alongside these remarkable developments, the ITU-AJ has been working hard to keep up with technological trends.

The ITU's most important decision-making event of the last year was the Plenipotentiary Conference in Dubai (United Arab Emirates). Japan was re-elected to the ITU Council, and Akira Hashimoto was appointed as a member of the Radio Regulations Board (RRB). In Japan, we held the International Conference for Cooperation on 5th Generation Mobile Communication Systems (ITU-R SG5 WP5D), and the ITU-AJ was able to participate in the administration of both conferences.

In South Africa, we prepared a report on the state of local telecommunications, which was delivered at ITU Telecom World 2018 in Durban. Also, on May 17 last year, we held the 50th Celebration of World Telecommunication and Information Society Day. At this event, Yuji Inoue received an award from the Minister of Internal Affairs and Communications in recognition of his work on international standardization at the ITU-T and other organizations, and Mahabir Pun received an ITU-AJ Special Achievement Award for the major contributions he has made to the construction of wireless communication technology in Nepal. Both awards were very richly deserved.

We also held an APT Training event for telecommunication engineers from developing countries around Asia, as well as our very popular "Performative Seminar", which we introduced into the curriculum of practical activities in order to improve international negotiating abilities.

This year, the World Radiocommunication Conference (WRC-19) will take place in Egypt for the purpose of discussing amendments to the radio regulations that govern the international allocation and use of radio frequencies. In addition, ITU Telecom World 2019 will be held in Hungary.

In Japan, we plan to hold a preparatory meeting (APG) ahead of this conference, and a meeting on standardization activities in the telecommunications field within the APT area (ASTAP).

I will be giving my full support to these activities alongside the Japanese government and our supporting members.

Finally, I'd like to wish you all a very happy New Year, and the best of success in your activities in 2019.

R&D Trends and Future Prospects of Quantum Cryptography

Masahiro Takeoka
Director
Quantum ICT Advanced Development Center, Advanced ICT Research Institute
National Institute of Information and Communications Technology

Mikio Fujiwara
Research Manager
Quantum ICT Advanced Development Center, Advanced ICT Research Institute
National Institute of Information and Communications Technology

Masahide Sasaki
Distinguished Researcher
Advanced ICT Research Institute
National Institute of Information and Communications Technology

1. Introduction

The information and communication technology that supports our modern network society has undergone remarkable development, and continues to advance every day. However, it has also been pointed out that the extension of conventional technology systems is liable to be impeded by the fundamental performance limits in the future. Quantum communication techniques exploit the properties of quantum mechanics (the physics of microscopic phenomena, such as the behavior of atoms, electrons, and photons) to their utmost potential. They are predicted to be used in variety of applications including unbreakable security techniques, ultra-long-range high-speed space communication, ultra-precise timing synchronization and sensing. As a result, the research and development of quantum communication is advancing all around the world. Although many of these are still at the stage of basic research, in this paper we introduce the current state of progress and the efforts being made in Japan and overseas with regard to quantum cryptography, which is one of the most mature applications in the field of quantum communications.

2. Quantum cryptography

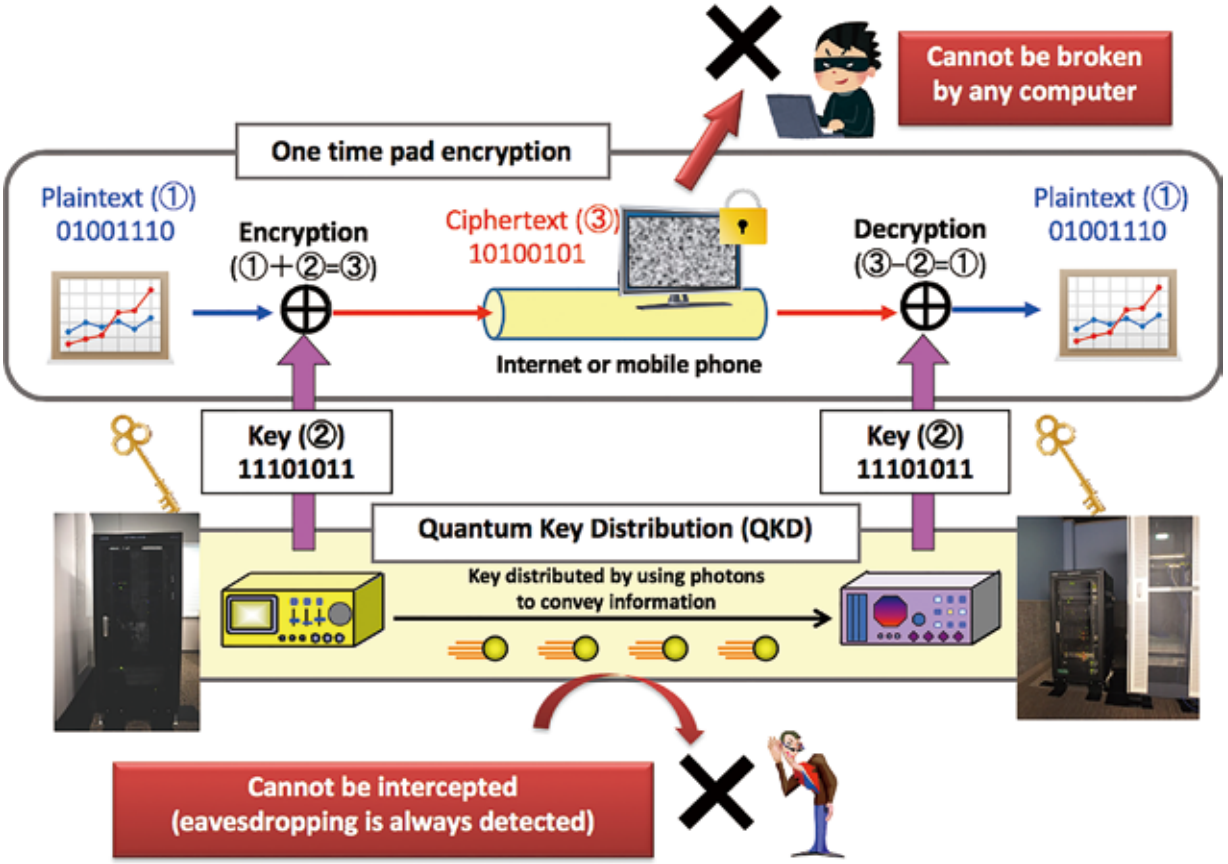
Cryptosystems based on mathematical algorithms such as RSA and elliptic curve cryptography are currently in widespread use throughout society. But although they are extremely easy to use, they are at risk of being broken by future developments in computer technology. The relationship between the performance of supercomputers and the amount of computation required to break RSA has already been estimated[1]. In addition, if recent rapid progress in R&D leads to the implementation of large-scale quantum computers, it could become possible to break these ciphers instantaneously. Furthermore, even if mathematical cryptosystems cannot be broken with existing computers, it is possible to intercept and store encrypted data so that it can be broken at a later date when sufficiently powerful computers have become available. This poses a serious potential threat to the communication of information such as state secrets and medical information (e.g. genomic data), which must provide the highest degree of security for many decades.

The security of quantum cryptography is not based on the difficulty of solving mathematical problems, but on quantum mechanics and statistics. As a result, quantum cryptography is the only current encryption method that is essentially impossible to break with computers of any kind, including quantum computers. This security is called "information-theoretic security" to distinguish it from computational security. In other words, if quantum cryptography is implemented appropriately, then it can provide absolute security that can never be broken regardless of future advances in computer technology and mathematics.

Figure 1 shows an overview of how quantum key distribution (QKD) is used to generate cryptographic keys in quantum cryptography, and how these keys are used to perform encryption*. In QKD, a random number that forms the basis of a key is delivered by transmitting a very weak optical pulse signal through

* There are several methods for encryption using keys created by QKD, but to achieve information-theoretic security, i.e. security unbreakable by any computing attacks, it is necessary to use "one-time pad encryption" where one data bit is encrypted using one key bit, and the same key bit is never used twice. Therefore, when we say that quantum encryption offers "perfect information-theoretic security," we are referring to the use of QKD + one-time pad encryption

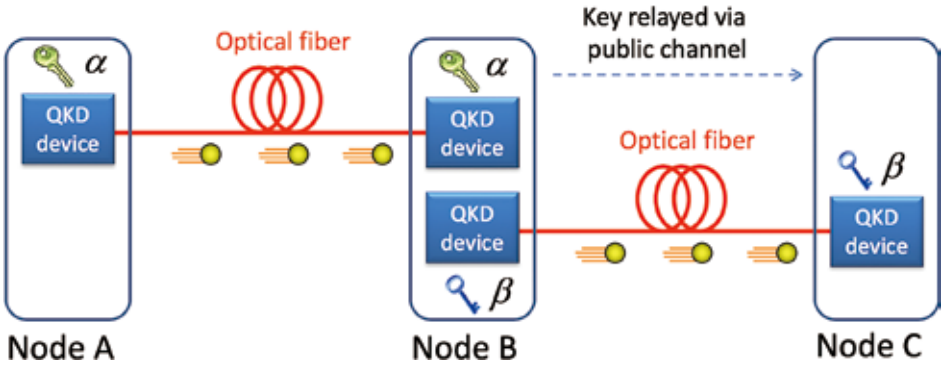
Figure 1: Overview of secure communication based on quantum cryptography (Photo: NEC's QKD transceiver)



a channel, typically an optical fiber, so that it contains on average only one photon (the smallest unit of light energy) per pulse (in standard optical communication, roughly 100,000 to 1,000,000 photons are contained in one pulse). The quantum nature of light is strongly apparent in a single-photon-level signal of this sort. One of the properties of QKD is that any attempt to eavesdrop by measuring signals en route will leave a detectable trace due to the uncertainty principle (one of the basic principles of quantum mechanics). As a result, it is possible to judge whether or not the signals have been tampered with, and to use only signals that are guaranteed not to have been intercepted. This allows keys to be shared with perfect security. Also, since the random number obtained as a key can be set to any desired sequence, one can use random numbers with no mathematical structure such as physical random numbers to make the key unbreakable by any computational attack. In this way, it is possible to detect any kind of physical eavesdropping during key distribution, allowing data to be encrypted with perfect security that cannot be broken by any computer. An actual QKD device consists of a photon transceiver combined with electrical components, e.g. a signal processing board that performs error correction and privacy amplification on the key information. The key itself is a binary sequence of zeros and ones, and after the key has been shared, it is used for data encryption/decryption and transmission via ordinary computers and communication channels, such as the Internet.

QKD overcomes the fundamental problem of mathematical cryptography, and can in some sense provide ultimate security. But on the other hand, there are also major restrictions on the implementation of QKD. Photons are easily lost due to transmission losses in communication channels, and it is not possible to use optical amplifiers (which are essential for long-distance fiber communication) because they destroy the quantum state of the signal. For this reason, the transmission range of a single QKD transceiver in fiber communication is limited to around 50 to 100 km. Furthermore, the key generation rate per wavelength is currently limited to the range of kilobits per second to megabits per second (depending on distance and device performances). It is expected that improvements will be made to some extent such as wavelength division multiplexing and other technical advances. A more fundamental challenge is to develop a novel technology called a "quantum repeater", which in principle can work as a repeater (amplifier) for quantum signals.

Figure 2: A QKD network where keys are relayed via trusted nodes



A quantum repeater must perform optical quantum computing on the transmitted signals, which is something that cannot be realized without further technological breakthroughs. Therefore, current QKD networks relay keys by connecting QKD paths between trusted nodes (i.e., nodes that are guaranteed to be secure; see Figure. 2). Although it is possible to construct a QKD network of any configuration in this way, the security of each relay station (trusted node) must be strictly guaranteed.

3. R&D trends in Japan and abroad

Thus, although quantum cryptography is still at a developmental stage, it is being actively researched and developed all over the world due to its ability to offer a level of security that is not attainable with conventional cryptography. This section introduces the R&D trends relating to the implementation of QKD in the field (for technical details and references, see, e.g. [2, 3]).

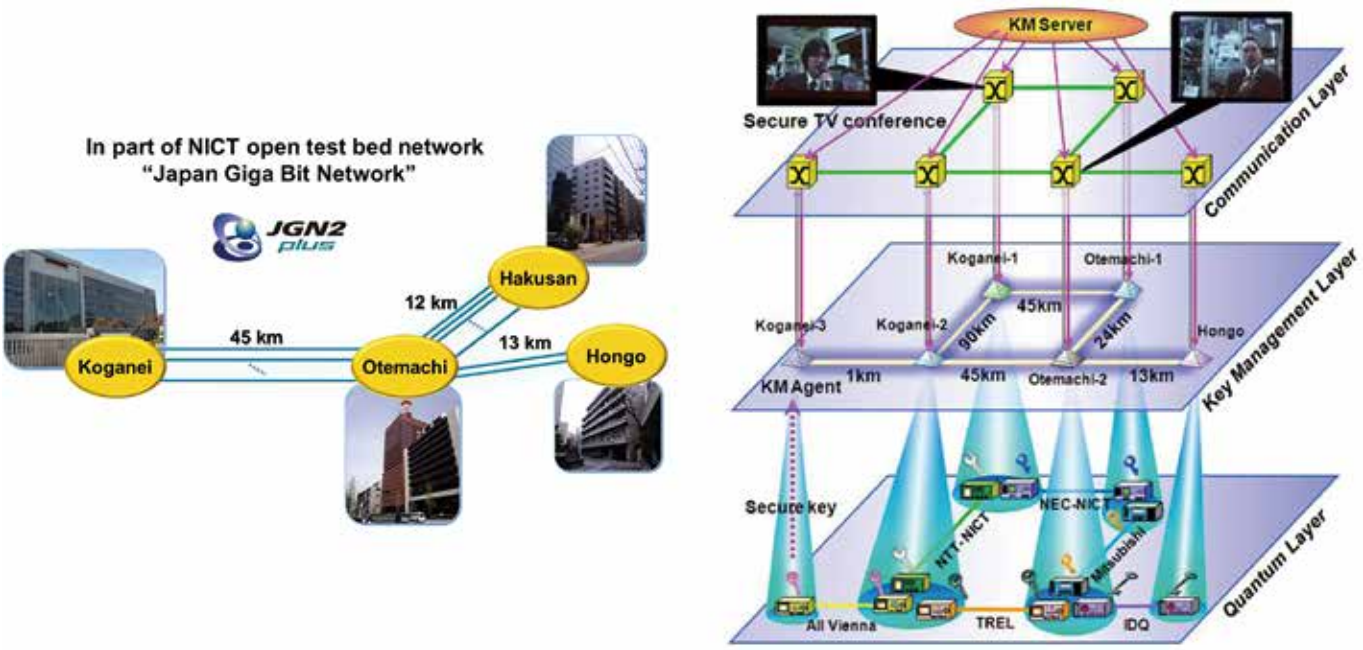
In 2004, using a terrestrial fiber-based QKD network, the Quantum Network project of the US Defense Advanced Research Projects Agency (DARPA) demonstrated the world's first metropolitan QKD network connecting three locations about 10 km apart in the Boston area. In 2008, the European Union's SECOQC (Secure Communication based on Quantum Cryptography) project set up a QKD network to connect six points in Vienna City, and they demonstrated that this allowed keys to be generated at about 1 kbps over a range of 30 km to support encrypted voice communication (phone lines) and other forms of encrypted communication. They also succeeded in interconnecting QKD devices based on different methods developed by multiple research organizations.

In Japan, the Ministry of Internal Affairs and Communications and the National Institute of Information and Communications Technology (NICT) have been promoting public–private collaboration projects, and in 2010, they built the Tokyo QKD Network from 100 kbps class QKD devices capable of generating keys a hundred times faster than earlier systems. As a result, they were able to perform the world's first demonstration of secure video transmission (video conferencing) based on QKD. Unlike the two earlier networks, the Tokyo QKD network remains operational to this day, and has been used to promote the development, trial operation and network testing of QKD devices developed by various Japanese research organizations. It is currently being used to transmit data for a distance of 50 km at approximately 1 Mbps, which is the world's highest performance for equipment deployed in the field. The project also developed QKD platform technologies, including key management platform technology for the secure and proper management of QKD networks and interfaces for supplying keys to the application layer in a suitable manner. These are necessary in practical applications of the QKD networks. QKD technology developed and tested in the Tokyo QKD Network has been deployed to actual user environments. Since 2015, NEC uses it to protect an in-house link between cybersecurity-related facilities, and Toshiba used it to protect the 7km data transmission link between the Toshiba Life Science Analysis Center and Tohoku University's Tohoku Medical Megabank Organization in Sendai.

Meanwhile, the progress made by China in recent years has been remarkable. Over a period of about three and a half years, China has constructed the world's largest QKD network connecting Beijing and Shanghai with 32 trusted nodes spread over a distance of about 2,000 km. This network has been operating since 2017. National projects to construct QKD networks are also under way in other countries including the UK and Italy, and quantum cryptography businesses in the US has announced plans to construct a QKD network service between Boston and Washington DC. In this way, the R&D and implementation of such networks remains competitive.

QKD can operate not only on optical fibers but also in free-space optical communication. For example, it is difficult to realize inter-continental ultra-long-distance key distribution (e.g., between Japan and the US) via a terrestrial QKD network connected via trusted nodes. However, the space environment of artificial satellites has a very thin atmosphere and can be used for communication with very low losses. Studies aimed at implementing satellite QKD are being pursued in several countries. In 2017, China succeeded in the first ever key generation by QKD between a satellite and a ground station. It also succeeded in key distribution via satellite between China and Austria, and demonstrated the encrypted transmission of a 5 kB image using this key. Meanwhile, in Japan, NICT is looking at

Figure 3: The Tokyo QKD Network (left) and QKD platform (right) constructed in 2010 [4]. See [5] for the current network operating status.



ways of implementing practical technology for the future, and has conducted a basic experiment (transmission and reception of weak photon-level signals) to demonstrate the world's first quantum communication using a microsatellite that has less than one tenth the mass of the Chinese satellite and is more cost-effective. Satellite quantum cryptography projects have been started in countries all over the world, and it is expected that competition in this field will become more intense in the future.

4. Integrating quantum cryptography with modern security technology: Data storage network based on QKD and secret sharing

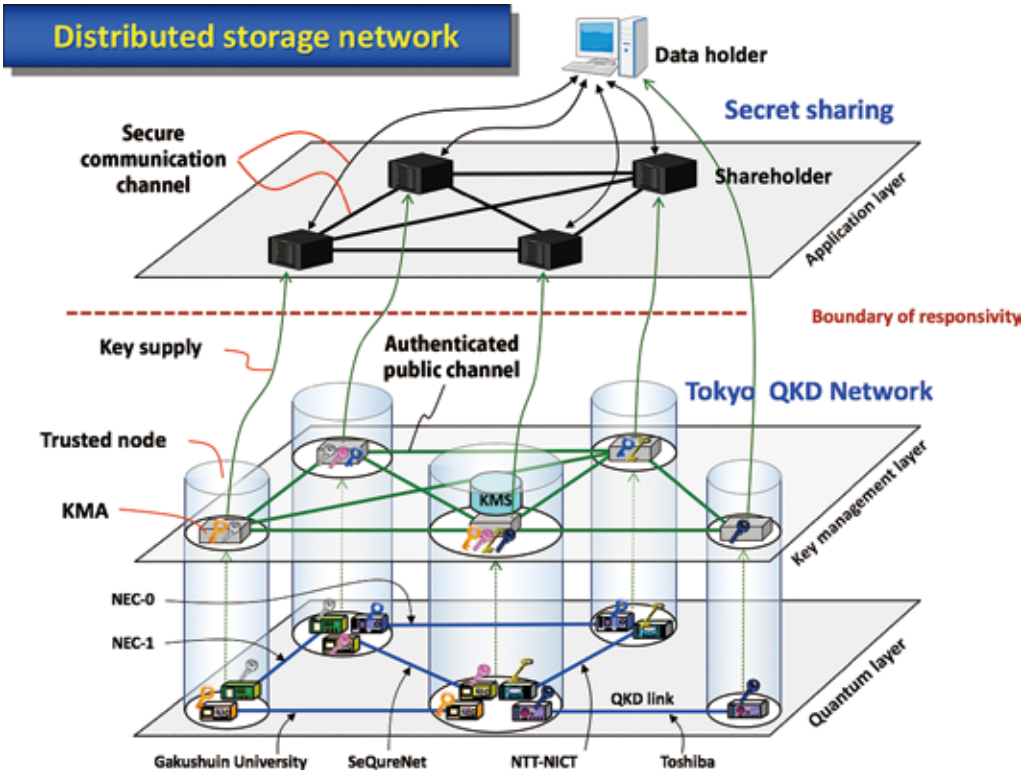
Although QKD guarantees unbreakable security during data transmission, it does not protect data in storage. However, in modern cryptography, there is a method called secret sharing whereby data is divided and encrypted before it is stored. For example, in Shamir's (n, k) threshold distribution method, the original data is divided into n shares that are separately encrypted. The original data can be restored by collecting k or more of these n shares, but with fewer than k shares, it is not possible to recover the original data using any computer; in other words, it has the information-theoretic security. Therefore, if data is distributed and stored in n separate locations, then it will still be information-theoretic secure even if part of it is stolen. Conversely, even if a part of the data is lost due to a natural disaster or the like, the information can still be recovered. This is an excellent mathematical algorithm that can be used to simultaneously save and backup secret data. However, it does not answer the question of how data shares can be securely transmitted to the distributed storage. In other words, if QKD and secret sharing can complement each other in the transmission and storage of data, then it will be possible to realize the security potential of secret sharing, resulting in a network that offers information-theoretically secure storage throughout the entire system.

Using five nodes on the Tokyo QKD Network, NICT and the Tokyo Institute of Technology have built a QKD secret sharing storage network that implements the secret sharing protocol described above. We also developed a protocol whereby information-theoretically secure authentication can be performed with a single password, and we were the first in the world to conduct a successful demonstration test of information-theoretically secure authentication, transmission, storage and recovery ([6] and section 3-2 of [2]). It is expected that this sort of distributed storage will be made publicly available in the near future as a way of creating backups to deal with disasters such as earthquakes and fires while at the same time providing the high level of security needed for confidential information such as medical records. If it is possible to construct a QKD network for distributed storage over an area of 50 to 100km, it would provide an effective system for storing secret backups that can withstand large earthquakes and tsunamis.

5. Standardization

Following the European SECOQC project, the European Telecommunications Standards Institute (ETSI) set up an Industrial Specification Group (ISG-QKD) to hold comprehensive discussions of QKD devices and to discuss details including the application interfaces and implementation security (security taking actual device performance and physical properties into consideration). Although the ETSI

Figure 4: A secret sharing storage network using QKD [2, 6].



has been actively working on QKD standardization for a long time, discussions of standardization have only started very recently at other standards organizations. This year, in the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T), study groups SG13 and SG17 issued proposals for technologies including a QKD network framework and network security. The International Organization for Standardization (ISO/IEC) has also produced a technical report on the subject. In China, a comprehensive framework for quantum communication technology is being discussed by the China Communication Standardization Association (CCSA). It is expected that active discussions and liaisons will continue in the future.

6. Conclusion

Although quantum cryptography cannot be deciphered by any computer and it can provide perfect security when properly implemented, it also involves practical difficulties such as high implementation costs and limitations in terms of distance and speed that do not apply to mathematical cryptosystems. For this reason, the social implementations of quantum cryptography are expected to start with high-end technology applications. Progress is also being made in the development of applications that uses technical components QKD, such as physical random number sources and key management/operation architectures. Meanwhile, mathematical cryptosystems are incorporating new technologies such as post-quantum cryptography which only provides computational security but is believed to be secure against attacks by quantum computers. Going forward, it will be essential to apply these various security technologies including quantum cryptography in an appropriate way by conducting R&D aimed at total solutions that provide the required security where it is needed in overall systems.

References

[1] CRYPTREC "Cryptographic Technology Evaluation Committee", 2013.

[2] "Special issue: Quantum data communication", Journal of National Institute of Information and Communications Technology, Vol. 64, No. 1 (2017).

[3] M. Fujiwara, A. Carrasco-Casad, T. Kitamura, M. Sasaki, M. Toshima: "Experimental optical communication between an ultra-small satellite and earth aiming for quantum communication", 38th Quantum Information Technology Study Group QIT2018–17, 2018.

[4] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD Network", Opt. Express, 19, 10387 (2011).

[5] The Project UQCC (Updating Quantum Cryptography and Communications). http://www.uqcc.org/

[6] M. Fujiwara et al., "Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing", Sci. Reports, 6, 28988 (2017).

Cover Art

Seki Sanjuro (Picture of kabuki actor Seki Sanjuro.)

Utagawa Toyokuni (1769-1825)

Collection of the Art Research Center (ARC)
Ritsumeikan University
Object number: arcUP3547

Trends in Post-Quantum Cryptography: Cryptosystems for the Quantum Computing Era

Naoyuki Shinohara
Senior Researcher
Security Fundamentals Laboratory
Cybersecurity Research Institute
National Institute of Information and Communications Technology

Shiho Moriai
Director
Security Fundamentals Laboratory
Cybersecurity Research Institute
National Institute of Information and Communications Technology

1. Introduction

Cryptography is one of the familiar basic technologies that supports modern society. For example, online retailers, card payments, travel cards and wireless LANs all depend on the use of cryptography. Today, RSA and elliptic curve cryptography (ECC) are the most widely used public-key cryptosystems. Quantum computers have been actively developed in recent years, and are expected to be used in a wide variety of fields. However, the development of large-scale quantum computers will cause a major reduction in the security of RSA and ECC. To address this issue, work is under way to develop and standardize post-quantum cryptography (PQC) technology that is secure against not only conventional computers but also quantum computers. This paper introduces the global trends in this field.

2. The impact of quantum computing on the security of current public-key cryptosystems

The security of public-key cryptosystems that are currently in use or under development is guaranteed based on the difficulty of solving particular mathematical problems by using computers. For example, in RSA (the most widely used public-key cryptosystem), two prime numbers of equal bit length are used as the private key, and the composite number obtained by multiplying them together is publicly distributed as the public key. Anyone who can decompose this composite number into its prime factors will be able to obtain the private key and break the RSA cryptosystem. Another widely used public-key cryptosystem is ECC, the security of which hangs on the difficulty of computing discrete logarithms on elliptic curves. That is, it is possible to obtain a secret key in this cryptosystem by solving a discrete logarithm problem on an elliptic curve. The ongoing development of quantum computers threatens the security of RSA and ECC because a quantum computing algorithm proposed by Peter Shor in 1994 can be used to solve integer factorization problems and discrete logarithm problems efficiently.

In experimental demonstrations of Shor's algorithm to perform integer factorization on a quantum computer, the current world record is the factorization of 21 (=3×7), so for the time being, quantum computers do not pose a serious threat to RSA or ECC. However, according to Internal Report 8105 published by the US National Institute of Standards and Technology (NIST) in 2016, it was stated that although it is not clear when scalable quantum computers will be implemented, quantum computer researchers estimate that quantum computers capable of factorizing 2048-bit RSA public keys may be built by 2030. Against this background, there is a need for cryptographic techniques that are secure against both conventional computers and quantum computers, and efforts are being made to rapidly develop and standardize post-quantum cryptography (PQC) techniques.

3. Development and standardization of post-quantum cryptography

Most of the cryptographic techniques currently in use took almost 20 years to gain widespread acceptance after they were first proposed. Since standardized post-quantum cryptography is expected to become available by 2030, it was therefore necessary to begin developing and standardizing post-quantum cryptography techniques from about 2010. Although post-quantum cryptography research and development has a long history, the first international academic conference focusing on post-quantum cryptography (PQCrypto) took place in 2006. The ninth PQCrypto conference was held in 2018, so it can be said that the development of post-quantum cryptography gained momentum just in time.

The domestic and international efforts to standardize PQC are introduced below (see Figure. 1). In 2015, the US National Security Agency (NSA) announced that it was planning to switch to post-quantum cryptography. The NIST also announced a call for proposals for post-quantum cryptography techniques in 2016, and by the November 30, 2017 deadline, they had received 82 submissions from around the world. 69 of these were announced as complete and proper submissions, and five were subsequently withdrawn (see Figure. 2). NIST is evaluating the candidate cryptosystems in terms of security, implementation performance and so on, and plans to release a draft post-quantum cryptography standard some time in 2022–2024. In Europe, the European Telecommunications Standards Institute (ETSI) is conducting surveys and other studies related to post-quantum cryptography. In the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC JTC 1/SC27 has started discussions aimed at the standardization of PQC.

Efforts to standardize post-quantum cryptography are also being made in Japan. Four organizations — the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, the National Institute of Information and Communications Technology (NICT) and the Information-technology Promotion Agency (IPA) — serve as the secretariat of the CRYPTREC (Cryptography Research and Evaluation

Figure 1: PQC standardization trends in Japan and overseas

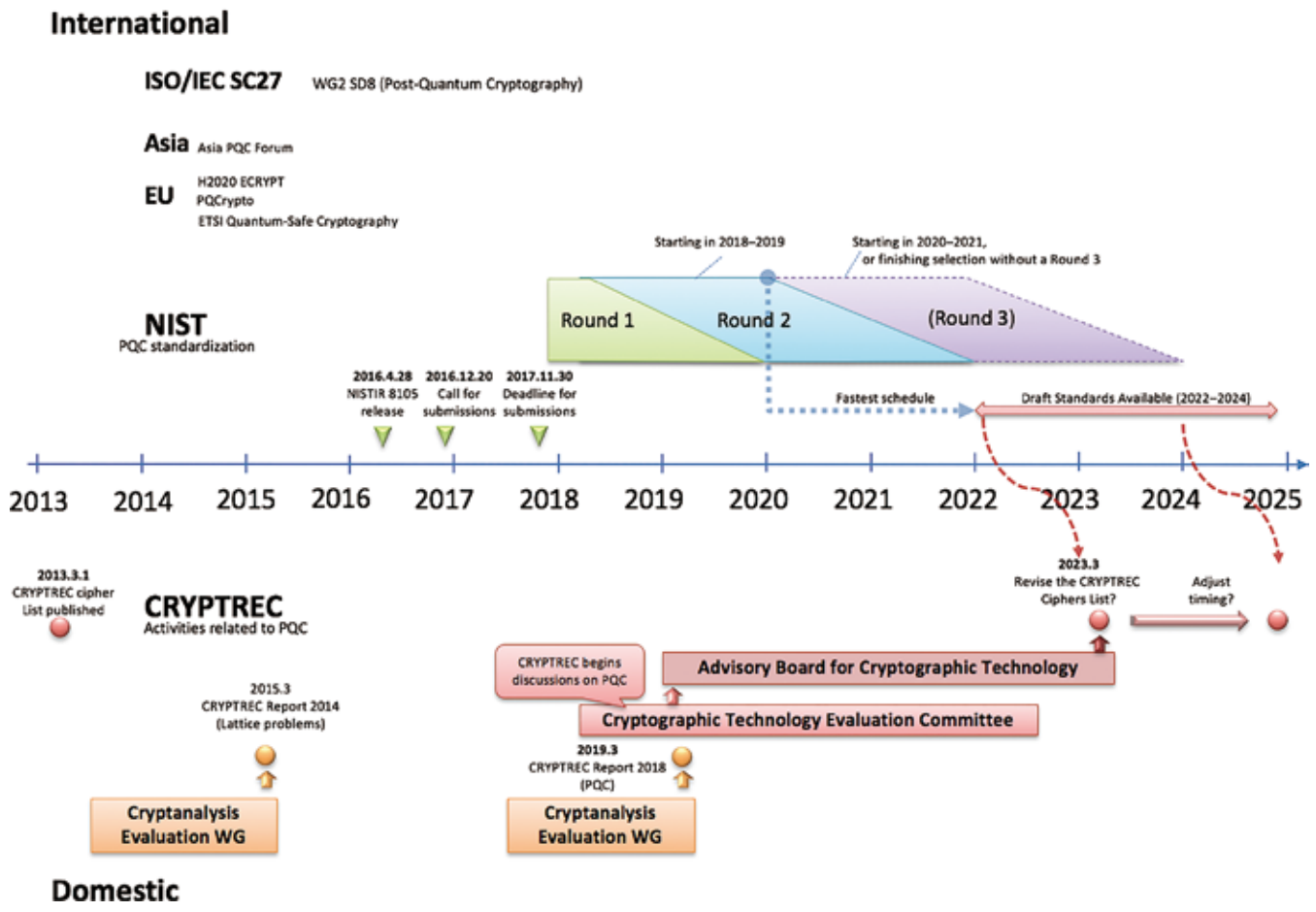
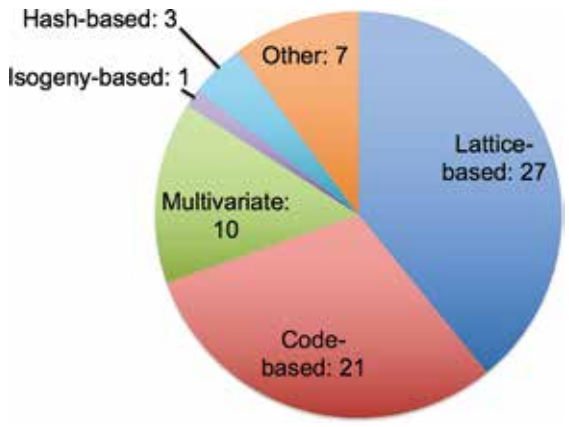


Figure 2: The 69 PQC candidates being considered for standardization by NIST(classified by base technology)



Committees) project, which evaluates and examines the security of a list of ciphers to be consulted by all government ministries when procuring information systems (the e-Government Recommended Ciphers List), and is conducting surveys and studies of appropriate methods for the implementation and operation of cryptography. Since 2014, with a view to standardizing post-quantum cryptography, we have been surveying research trends regarding lattice-based cryptography (a promising candidate for post-quantum cryptography), and the mathematical problems related to the security of this technique (lattice problems), and we have published technical reports summarizing our findings. Besides lattice-based cryptography, there are several other promising candidates for post-quantum cryptography. These include code-based cryptography, multivariate cryptography, and isogeny-based cryptography. At CRYPTREC, we have been surveying these four post-quantum cryptography techniques since 2017, and in 2019 we plan to publish a technical report summarizing our findings.

4. Development of the LOTUS post-quantum cryptosystem at NICT

NICT has spent many years developing cryptographic techniques and researching the evaluation of their security. Regarding post-quantum cryptography, we developed a new

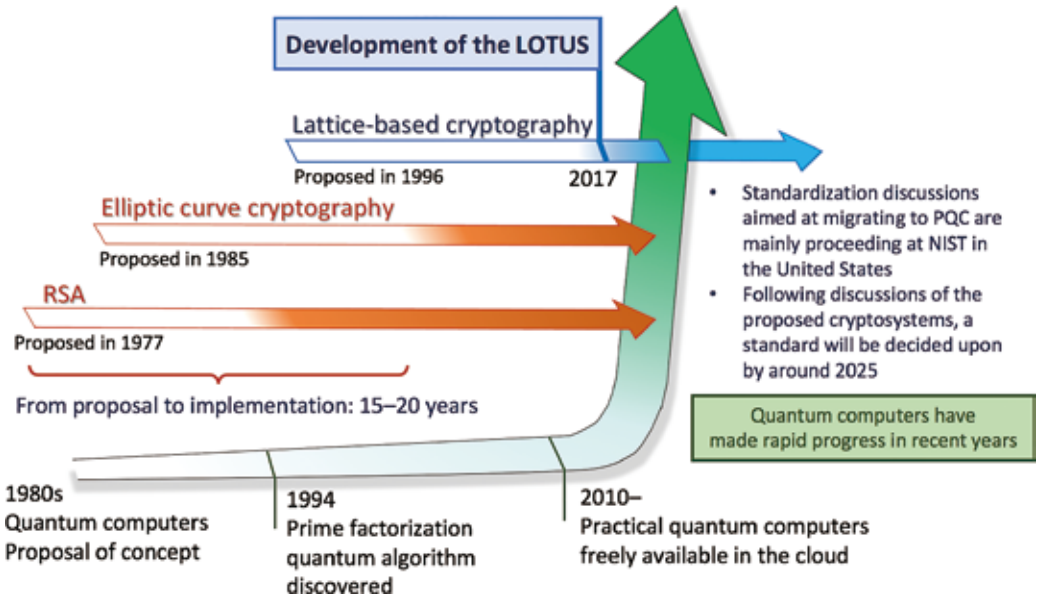
lattice-based public key cryptosystem called LOTUS, which we proposed to NIST's post-quantum cryptography standardization project in 2017 (see Figure. 3). This scheme was announced as a complete and proper submission, and so far, no major security flaws have been discovered. The evaluation of this scheme as a candidate for standardization is continuing.

LOTUS is not only secure against quantum computers, but also has versatility, making it suitable for use in wide range of applications including web browsers and databases. Versatility is a concept related to the overall security of a cryptosystem comprising a combination of multiple cryptographic techniques. Cryptographic techniques must first of all be individually secure. Furthermore, when they are used in practice, they may be combined with other cryptographic techniques. It is necessary that these combinations do not give rise to vulnerabilities. When combining cryptosystems that lack versatility, it is generally difficult to guarantee the security of entire system, even if each component is secure.

When using a cryptosystem that lacks this property, any mistakes made when combining these elements is liable to introduce vulnerabilities capable of being exploited by an attacker, and the entire system will be at risk of being broken. Guaranteeing the security of the entire system involves a two-step procedure where the security of each individual cipher is first proved, and then the security of the whole cryptosystem is proved. However, it can take experts several days to verify a complicated system, and this complexity can also cause problems such as an increased likelihood of errors. At the design stage of a cryptosystem, the property of versatility makes it possible to avoid such dangers. The security of a system that combines cryptosystems with versatility can be proved mathematically, which means the step of proving the overall system's security can be omitted. In the LOTUS system developed at NICT, we have added data corruption resistance to the basic lattice cryptography by incorporating a mechanism that checks the structure of ciphertexts when they are decrypted. This checking mechanism has been mathematically proven to have versatility that allows it to be combined with other cryptosystems, which means this cipher can be used in diverse situations in society by incorporating it into various different systems.

At the same time, we have also developed a security evaluation method for lattice-based cryptosystems, which has made it possible to set parameters suitable for long-term use of the cryptosystem. Since this security evaluation method can also evaluate other lattice-based cryptosystems, we now believe it can contribute to fair security evaluations by providing a unified basis for the evaluation of proposed candidate systems in the NIST standardization project.

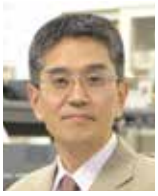
Figure 3: The LOTUS



Initiatives for New Computers using Quantum Technology

Shiro Saito
Group Leader
Superconducting Quantum Circuit Research Group
Physical Science Laboratory, NTT Basic Research Laboratories
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

Hiroki Takesue
Group Leader
Quantum Optical State Control Research Group
Optical Science Laboratory, NTT Basic Research Laboratories
NIPPON TELEGRAPH AND TELEPHONE CORPORATION



Hideki Gotoh
Executive Manager
Research Planning Section, NTT Basic Research Laboratories
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

Advances in current digital computer technology are appearing to approach saturation, and there is much active R&D on computers that use physical systems to solve problems more efficiently than existing computers. Quantum computers are attracting attention in this research, as a technology that can dramatically increase efficiency in terms of computing time and energy consumed relative to conventional computers by using quantum superposition states. Recently, large enterprises such as IBM, Google, and Microsoft are putting great effort into developing quantum computers. This article introduces initiatives at NTT to implement new computing devices using physical systems. Section 1 discusses a new type of computer called a Coherent Ising Machine (CIM), which uses quantum electronics technology developed at NTT. Section 2 introduces experiments demonstrating quantum mechanical principles using qubits, which are the basic device used in the quantum computer.

1. New theoretical computer using light: the "Coherent Ising Machine"

NTT is conducting R&D on a computer called a Coherent Ising Machine (CIM), based on new principles. A CIM uses quantum electronics technology and is able to solve combinatorial optimization problems efficiently. It uses a type of oscillator called a degenerate optical parametric oscillator (DOPO), which is able to solve Ising model energy-minimization problems rapidly. The Ising model is a theoretical model of a set of interacting atomic spins.

A DOPO is a special type of optical oscillator for which, above the oscillation threshold, the oscillation phase can only take one of two values, 0 or π, relative to the phase of the pump beam/light, which is described below. Thus, by assigning a phase of 0 to up-spin and π to down-spin, the DOPO phase can be a stable expression of the Ising spin state. A DOPO is generated by placing a special type of optical parametric amplifier called a phase-sensitive amplifier (PSA)[1] in the optical oscillator. When a pump wave and a signal wave are injected into a non-linear optical medium, the PSA amplifies the signal wave and also generates an "idler" wave, which has a frequency corresponding to the difference between the signal wave and the pump wave. Here, if the signal and idler waves have the same frequency, the amplifier efficiency is maximized for signals with phase of 0 or π relative to the pump wave. Placing a PSA in the optical oscillator creates an oscillator that only oscillates at phases of 0 or π relative to the pump wave.

A single optical system with N independent DOPO pulses can be generated by using a pulsed-state pump wave with this optical oscillator, and setting the period of the optical oscillator to N-times the interval of the pump wave pulses[2]. NTT has successfully generated sets of 5000 to 1 million time-multiplexed DOPO pulses using optical oscillators of lengths from 1 to 20 km and pump wave pulses with feedback frequencies from 1 to 10 GHz[3-6].

Interaction between DOPO pulses has been reported earlier, using a direct coupling method with a delay-interferometer[2,3], and a measurement-and-feedback (MFB) method[5,6]. Here we discuss a method using MFB. A schematic diagram of a CIM using MFB is shown in Figure 1. A PSA in a 1-km optical fiber oscillator is driven with pump wave pulses repeating at a frequency of 1 GHz, which generates a set of approximately 5000 DOPO pulses. When the pump wave is input to the PSA, a noise wave pulse called a squeezed vacuum wave is generated, which then circles the oscillator, and the pulse is amplified gradually by repeated PSA amplifications. After approximately 1000 cycles, DOPO characteristic phase separation occurs. At this point,

a beam splitter is used to extract some of the energy of a 2048 DOPO pulse set in each cycle of the DOPO oscillator, and the amplitudes are measured using a balanced homodyne detector. The result of measuring these amplitudes (a 2048 element vector) is input to a field programmable gate array (FPGA). The spin interactions representing the Ising model problem to be solved (a 2048x2048 matrix) are input to the FPGA ahead of time. By computing this product, the FPGA produces feedback signals for each DOPO pulse, to implement the desired connections. Coupling between DOPO pulses is achieved by using the optical modulator to inject optical pulses with the same frequency as the DOPO pulses into the oscillator, superposing them on the DOPO pulses. Using this method, we were able to realize two-body interactions for all combinations among 2000 spins (approximately 4 million, including directed couplings). The set of vacuum squeezed optical pulses initially has random phases but with repeated MFB interactions, the entire system quickly settles to a combination of phases that is optimally stable. The solution to the input Ising problem is obtained by reading out the phases of each DOPO pulse after oscillation.

With collaboration from NII, Osaka University, and Tokyo University, NTT has built an MFB-based CIM and used it to search for solutions to large-scale combinatorial optimization problems (Figure 2)[5]. In experiments conducted in 2016, we searched for a solution to a fully-connected graph max-cut problem with 2000 elements and achieved an equivalent solution approximately 50 times faster than a CPU implementation of simulated annealing,. NTT is currently developing CIM equipment that is more compact and has stable operation over longer periods of time under the technology brand name "LASOLV", and is engaging in R&D to apply it in society.

Figure 1: CIM configuration
(from NTT Technical Journal Vol. 2017.5, pp. 11-14, 2017)

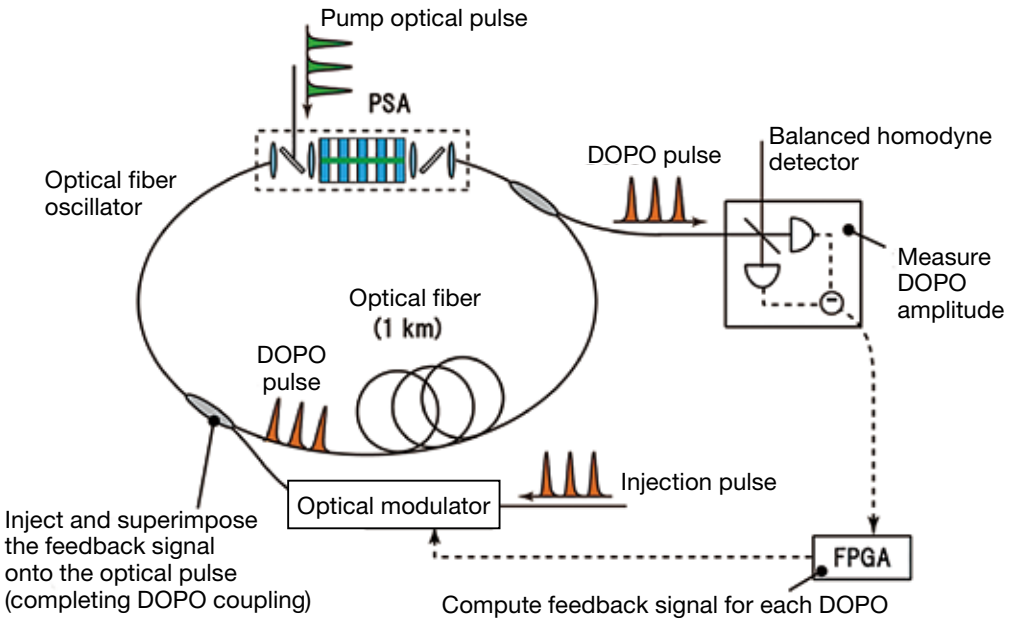
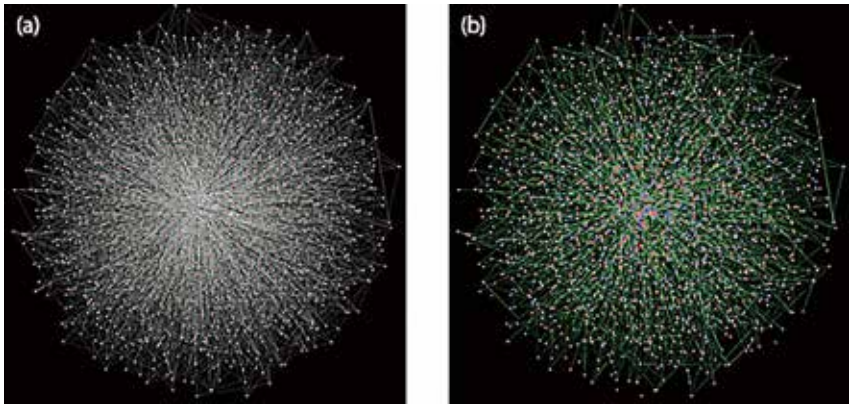


Figure 2: Using the CIM to solve a max-cut problem. (a) Visualization of a graph problem with 2000 vertices and 19900 edges. Vertices are shown as pink dots and edges as white lines. (b) Solution found by the CIM. Vertices are partitioned into red and blue groups, and edges shown in green are cut. (from NTT Technical Journal Vol. 2017.5, pp. 11-14, 2017)



2. Demonstration of quantum mechanical principles using a quantum bit

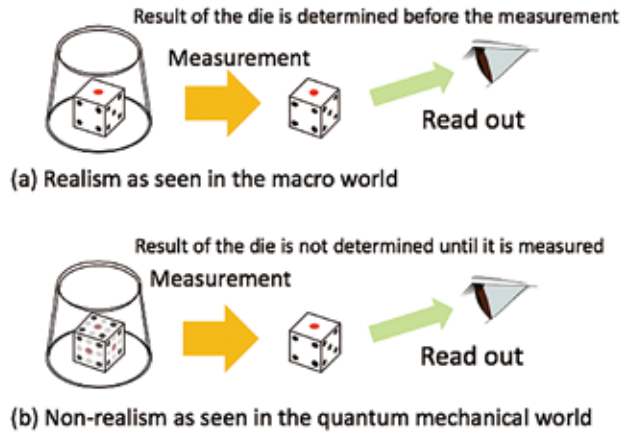
Ion-trap quantum computers and superconducting quantum bits are technologies attracting attention for realizing quantum computers. The former uses the microscopic physical system of a natural atom as a quantum bit, so it is isolated from surrounding noise and has the long coherence times necessary for quantum computations. In contrast, the latter uses circuit elements such as capacitors, inductors and Josephson junctions, so circuits can be designed freely and are very extendable and controllable. However, superconducting quantum bits are created with semiconductor nano-fabrication processes and are macroscopic physical systems (several μm) compared to atoms, so they are susceptible to the effects of noise and have short coherence times. Coherence characteristics have been improved dramatically recently, using circuit design techniques, achieving gate fidelity comparable to ion traps, but a huge amount of effort has been invested in improving coherence characteristics in superconducting quantum bit research in the past 20 years. In this process, NTT has used the fact that superconducting quantum bits are a macroscopic system to investigate the scale to which quantum mechanics can be applied, which has been a fundamental question since quantum mechanics was discovered.

Realism and Non-realism

Consider an experiment in which a die is placed in a cup and shaken. If the cup is opened and the die shows one dot, we assume that the die showed a one, even before the cup was opened. We assume, when we observe an object in a particular state, that it was in that state before the observation and that the observation did not affect the state. This way of thinking is referred to as "realism" and is taken for granted in everyday life (Figure 3(a)).

However, according to quantum mechanics, objects exhibit strange states called "superposition states," which are contrary to everyday common sense. Consider the example of a quantum die in Figure 3(b), conforming to quantum mechanics. A superposition state with the die showing values from 1 to 6 with equal probability exists in the cup, and the moment the cup is opened and observed, one of these states is decided. This property, in which the state is not determined before the observation, and only determined by the fact of the observation, is called "non-realism," and is known to occur in microscopic systems (atoms, electrons, etc.) conforming to quantum mechanics. Of course, it is not possible to verify non-realism using macroscopic objects like dice, but the question of the scale of macroscopic objects to which quantum mechanics can be applied is very interesting.

Figure 3: Realism and non-realism



Preparing macroscopic systems

In 1985 Professor Anthony Leggett from Illinois University predicted a superconducting ring with Josephson junctions could realize a state with currents flowing in the ring in both clockwise and counter-clockwise directions, and published a paper showing how to demonstrate that non-realism can occur in macroscopic systems[7]. Later, as interest in quantum computers increased, superconducting circuits were developed, and a superconducting ring with three junctions became established as the superconducting flux quantum bit (Figure 4(a)). When magnetic field through the ring approaches a half-integer multiple (…-0.5, 0.5, 1.5, …) of a flux quantum, Φ_0, the state of the current flowing clockwise (or counter-clockwise) in the flux qubit stabilizes. Worth mentioning is that the size of the flux qubit (several μm) is very large compared to electrons and atoms, and the current (several 100 nA) amounts to a flow of a trillion electrons per second. NTT has verified quantum superposition states in these currents, which are macroscopic physical quantities, and aimed to verify non-realism properties in them.

Verification of non-realism

Prof. Leggett proposed a thought experiment in which the state of current flow in a superconducting ring is measured at several times. It indicated that if measurements could be made without disturbing the state and realism is established, then a correlation between the measured values would verify that the Leggett-Garg inequality is satisfied. That is to say, if it could be shown that this inequality is violated when making measurements that do not disturb state, then non-realism would be demonstrated, and subsequently quantum mechanics would apply to the system. At NTT, we have derived conditions that are mathematically equivalent to this inequality, and used the following method to verify non-realism experimentally[8].

If a flux qubit conforms to quantum mechanics, then a quantum superposition state, $|-1\rangle+|1\rangle$, will be realized when it is exposed to a microwave equivalent to the energy difference between the two-current states, $|-1\rangle$, $|+1\rangle$, for a suitable amount of time. When this microwave irradiation is repeated four times, the state returns to its original state, as shown in Figure 4(b), so this exposure to microwaves is called a state operation ($\theta=\pi/2$). This state operation is used to conduct the two experiments shown in Figure 4(c). A flux qubit with state $|-1\rangle$ is first prepared, and after repeating the state operation twice, and readouts of the final state are compared. The difference is that between the state operations, a measurement is taken or not. If realism is true, then the state before and after the measurement will not change, so no difference will appear between the two tests, and the difference d_P between the read-out expected values $\langle Q_3 \rangle$ will be 0.

Next, consider the case where non-realism is shown

establishing that quantum mechanics applies. In the second experiment in Figure 4(c), after applying the operation twice, the initial value of |-1> will become |1>, and the expected readout value will be 1. Conversely, in the first experiment, a measurement is taken after the first state operation, on the superposition state |-1> + |1>. With this observation, a probabilistic quantum projection to |-1> or |+1> occurs, so the next operation produces a superposition state of |-1> + |1> or |-1>-|1>. When this is read out, the expected value is 0 in both cases. Thus, the difference in expected values for the two experiments, $|d_\rho|$, is 1. In the actual experiment, there are limitations on the precision of the readout, so $|d_\rho|$ is a finite value less than 1. From the discussion above, we expect that if realism holds true, d_ρ=0, and if non-realism holds true, $|d_\rho|$>0. We refer to this as the main experiment.

Note that ideally, our main experiment is conducted using "non-disturbing measurements", but noise and imperfections in measurements results in a small amount of disturbance to the state. To evaluate this quantitatively, we also conducted a control experiment. We prepared pure |-1> or |+1> states with no superposition after the first state operation and then evaluated the difference in readout results with and without a measurement. Here, when preparing |-1⟩ and |+1⟩ states, the expected differences in readout are defined as d_g and d_e respectively. Ideally, d_g=d_e=0, but small variations are generated due to disturbance of the state by the measurements. Results of this experiment are shown in Figure 4(d). d_ρ greatly exceeds the values between d_g and d_e, indicating that the behavior of the flux qubit cannot be explained by realism, and that non-realism holds true. The separation of d_ρ from d_g and d_e is approximately 84 times the standard deviation of experimental error, verifying that quantum superposition states were realized in the flux qubit, and that quantum mechanics holds true for this macroscopic system.

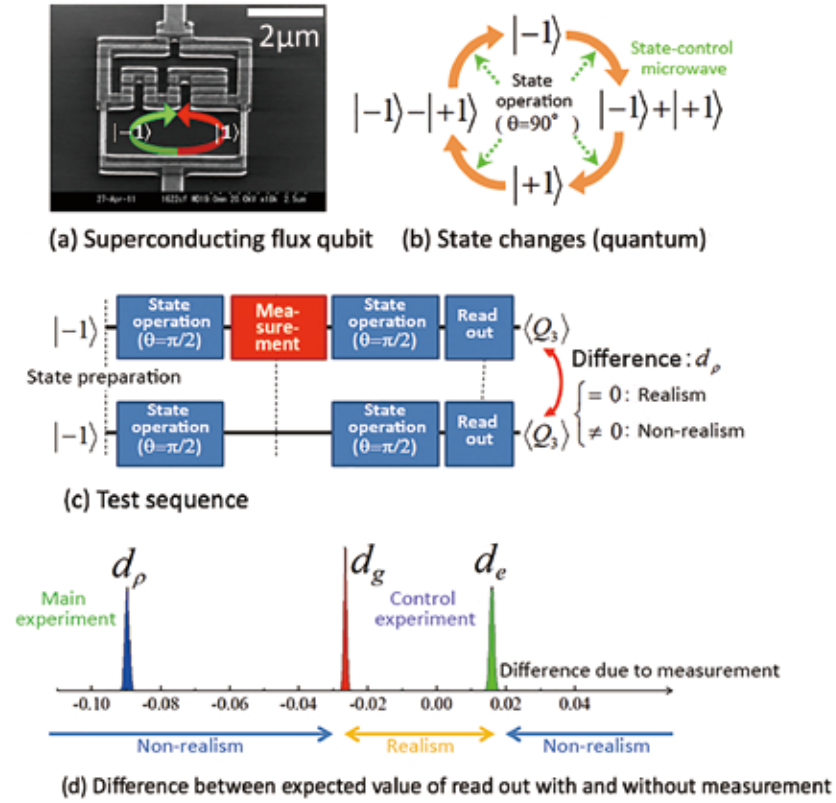
3. Conclusion

In the first part of this article, we introduced the CIM, which is a new type of non-Von Neumann computer that surpasses conventional computers in solving particular optimization problems. We intend to increase the scale of this system and use it to solve problems in real society in the future.

In the second part, we showed how quantum superposition states, a basic quantum mechanical property which had only been verified at the microscopic scale of individual electrons and other atomic particles, can also be seen in macroscopic currents flowing in a superconducting ring on a scale that can be observed using an optical microscope. We hope to verify non-realism at even larger scales in the future.

References
[1] T. Umeki, M. Asobe, and H. Takenouchi, Opt. Express 21, 12077 (2013).
[2] A. Marandi, Z. Wang, K. Takata, R. L. Byer, and Y. Yamamoto, Nat. Photon. 8, 937 (2014).
[3] T. Inagaki, I. Inaba, R. Hamerly, K. Inoue, Y. Yamamoto, and H. Takesue, Nat. Photon. 10, 415 (2016).
[4] H. Takesue and T. Inagaki, Opt. Lett. 41, 4273 (2016).
[5] T. Inagaki, Y. Haribara, K. Igarashi, T. Sonobe, S. Tamate, T. Honjo, A. Marandi, P. L. McMahon, T. Umeki, K. Enbutsu, O. Tadanaga, H. Takenouchi, K. Aihara, K. Kawarabayashi, K. Inoue, S. Utsunomiya, and H. Takesue, Science 354, 603 (2016).
[6] P. L. McMahon, A. Marandi, Y. Haribara, R. Hamerly, C. Langrock, S. Tamate, T. Inagaki, H. Takesue, S. Utsunomiya, K. Aihara, R. L. Byer, M. M. Fejer, H. Mabuchi, and Y. Yamamoto, Science 354, 614 (2016).
[7] A. J. Leggett and A. Garg, Phys. Rev. Lett. 54, 857 (1985).
[8] G. C. Knee, K. Kakuyanagi, M-C. Yeh, Y. Matsuzaki, H. Toida, H. Yamaguchi, S. Saito, A. J. Leggett, and W. J. Munro, Nat. Comm. 7, 13253 (2016).

Figure 4: Test method and results



Development of a Combinatorial Optimization Calculation Engine

Takayuki Shibasaki
Research Manager
Digital Annealer Project, Technical Development Group
Fujitsu Laboratories LTD.

1. Introduction

It is said that improving performance in semiconductor integrated circuits through scaling is slowing down and will essentially come to an end in several years[1]. One means of improving performance without depending on scaling is to employ specialized domain-specific hardware, but this creates another problem in that increasing the degree of specialization narrows the application area making it difficult to recoup development costs. It is therefore important to focus on domains that can be applied as much as possible to a broad range of fields.

The need for selecting an optimal combination from among many combinations is present in a variety of fields. In general, the time needed to solve a combinatorial optimization problem increases dramatically as the scale of the problem grows, and as a result, conventional computers are limited in the scale that they can handle. Against this background, we have developed Digital Annealer, an optimization calculation engine for solving combinatorial optimization problems. This paper describes Digital Annealer architecture and introduces acceleration and scaling technologies.

2. Digital Annealer architecture

2.1 Search technique using the Ising energy function

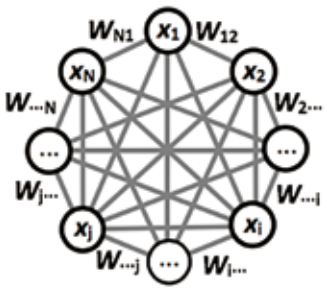
Digital Annealer performs statistical searching in parallel based on a Markov Chain Monte Carlo method (MCMC), which entails minimizing the Ising energy function shown by Eq. (1) at high speed.

$$E(X) = -(1/2)\sum_{i,j} W_{ij}\, x_i\, x_j - \sum_i b_i\, x_i \qquad (1)$$

$$x_i \in \{0,1\}\ (i = 1, 2, \cdots, N),\ W_{ii} = 0,\ W_{ij} = W_{ji}$$

Here, X is a set of bits with $X = (x_1, x_2, \ldots, x_N)$. N bit values x_i, $(i = 1, 2, \cdots, N)$ expresses a combination. W_{ij} denotes the combination coefficient between bit i and bit j and b_i is a bias term with respect to each bit. Digital Annealer features a full-connection architecture that can express mutual interaction among all bits (Figure 1).

Figure 1: Schematic of full-connection structure



2.2 Acceleration by parallel trials

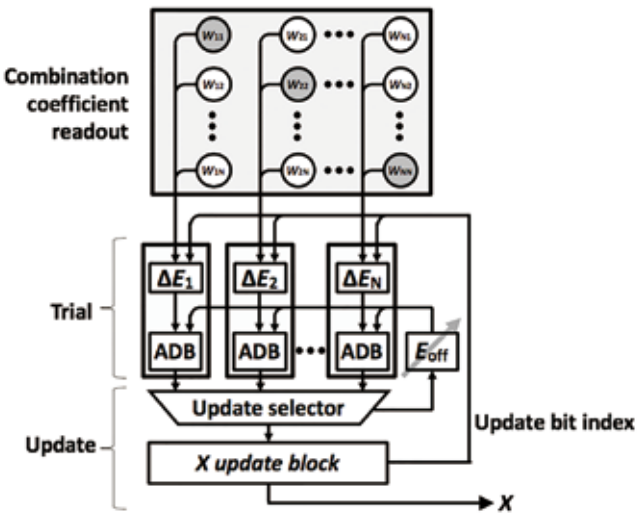
The operating cycle of the Digital Annealer is divided into two phases: the trial phase that selects bit inversion so as to satisfy an acceptance criterion and an update phase that inverts the selected bit (Figure 2).

The trial phase takes the current bit set $X = (x_1, x_2, \ldots x_N)$ and inverts a single bit value x_i to 1- x_i to obtain N-element neighboring state $X^{(i)}$ to be examined. Letting ΔE_i denote the increase in energy $E(X)$ obtained by making a transition from current state X to neighboring state $X^{(i)}$, the Metropolis-Hastings criterion given by Eq. (2) is used to decide whether to accept the bit inversion.

$$A(\Delta E_i) = \min[1, exp(-\beta \Delta E_i)] \qquad (2)$$

Here, $A(\Delta E_i)$ denotes the inversion-acceptance probability for energy change ΔE_i when inverting bit x_i to 1-x_j and β (=1/T) is the reciprocal of temperature T used in the simulated annealing method. Now, an Acceptance Decision Block (ADB) established for each bit compares the value of ΔE_i for each state change with an appropriate random number (noise) and outputs a binary flag that takes on the value of 1 with the acceptance probability of Eq. (2). A value of 1 for this binary flag means that inverting the corresponding bit is good. Finally, the update selector selects a

Figure 2: Digital Annealer configuration



single bit to be inverted based on those bits whose binary flags took on the value of 1. If there is no bit candidate for updating, the update selector outputs a flag with the value 0.

Here, we explain why the parallel trials scheme results in high-speed processing compared with conventional MCMC. Given the system in state X, let P_{single} denote the probability of making a transition to some new state for the case of a single trial in ordinary MCMC. Denoting the increase in energy when making a transition to neighboring state $X^{(i)}$ as ΔE_i, P_{single} is given by Eq. (3) using the transition-acceptance probability of Eq. (2).

$$P_{single} = (1/N) \sum_{i=1}^{N} A(\Delta E_i) \quad (3)$$

The probability of selecting a specific bit i is uniformly 1/N and the probability that an inversion can occur when that bit is selected is $A(\Delta E_i)$. Consequently, since any bit is fine, the probability that an inversion can occur is given by Eq. (3).

We now determine probability $P_{parallel}$ of making a transition to a new state under the parallel trials scheme of Digital Annealer. Here, we assume the selection rule that one bit out of N bits is selected with the probability given by Eq. (3). Now, considering that the probability of discovering a state as a transition destination is small when approaching an optimal solution so that $A(\Delta E_i) \ll 1$ (i=1, 2, ⋯, N), we get:

$$P_{parallel} = 1 - \prod_{i=1}^{N}(1 - A(\Delta E_i)) \cong \sum_{i=1}^{N} A(\Delta E_i) = N \cdot P_{single} \quad (4)$$

Equation (4) shows that the probability of making a transition to a new state in the case of parallel trials is N times that of the single search scheme. This technique is also advantageous in that no convergence problem occurs, which differs from a parallel trials scheme that simply updates multiple bits in parallel.

2.3 Acceleration by offset addition

If the state of a system falls into a local minimum of the Ising energy function, the probability of exiting that state into another one may be quite low even if using parallel trials. In such a case, the system will stay at the same local minimum for some number of cycles adding to the time taken until convergence. To therefore decrease the time stuck in a local minimum, we implemented a means of subtracting a positive offset E_{off} from the energy increment. This is practically equivalent to multiplying the common factor $\exp(\beta \cdot E_{off}) > 1$ by the acceptance probability of state inversion. To execute this, we add a fixed incremental value to the offset using an offset generator whenever a new candidate for bit inversion cannot be found and continue increasing the offset until the next state is found. This method dynamically controls the offset value so that the probability of finding the next destination for state inversion is 1 thereby shortening the time stuck in a local minimum.

2.4 Exchange Monte Carlo Method

There are a variety of acceleration techniques in stochastic searching using replicas. The simplest of these techniques is simple parallel operation, which gives the same problem to multiple replicas and performs statistically independent searches. Given M replicas, let the state vector of those replicas with the lowest objective function (energy) be the solution. Now, denoting the accuracy rate of individual replicas when annealing each replica for a certain number of cycles as P_0, accuracy rate P_{total} (M) for all M replicas can be given by Eq. (5).

$$P_{total}(M) = 1 - (1-P_0)^M \quad (5)$$

Thus, to obtain a total accuracy rate P_{total} (k) of 99%, the accuracy rate P_0 of individual replicas must be P_0=0.99 for M=1, P_0=0.37 for M=10, and P_0=0.045 for M=100. The time required (number of cycles) to obtain a correct answer becomes shorter by the amount deemed acceptable in making the target accuracy rate of individual anneal blocks smaller.

A serious problem in the simulated annealing method is that the state vector can become stuck near a local minimum as the temperature drops thereby slowing down the process of arriving at a true solution. This is known as the "hardly relaxing" problem in simulated annealing[2]. While Digital Annealer achieves high-speed processing by shortening the average trial time, it does not in essence solve the "hardly relaxing" problem. In addition, simple parallel operation as well cannot solve this problem.

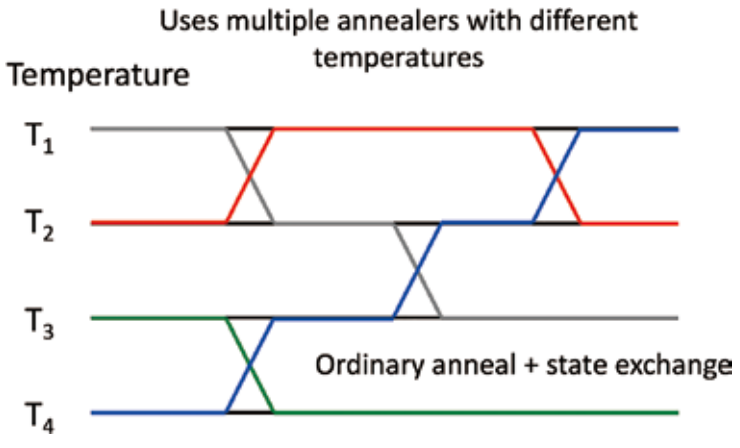
In the field of statistical physics, methods for solving the "hardly relaxing" problem were first devised in the mid-1990s. These methods conduct a stochastic search using multiple statistical ensembles (replicas) having different parameters (such as temperature). The exchange Monte Carlo method is one such method that uses multiple replicas[3]. This method prepares M replicas with different temperatures ($T_1 > T_2 > \cdots > T_{Ne}$) and conducts a stochastic search on each. It also exchanges state vectors between replicas with adjacent temperatures under certain conditions (using the Metropolis flow rule). Exchanging states in this manner can create a path between low-temperature replicas (that easily fall into "hardly relaxing") and high-temperature replicas (that have no "hardly relaxing" problem) and thereby solve the "hardly relaxing" problem overall (Figure 3). Digital Annealer supports both simple parallel operation and the exchange Monte Carlo method.

3. Scaling technologies

3.1 Approaches to scaling up

Problems of increasingly larger scale must be supported to expand the application domain of Digital Annealer. We have therefore been engaged in the ongoing development of scaling

Figure 3: Stochastic searching by the exchange Monte Carlo method



technologies from both hardware and software perspectives. At present, the number of bits *N* that can be handled by first-generation Digital Annealer hardware is 1,024 bits. To begin with, we will expand *N* in second-generation Digital Annealer hardware to 8,192 bits. Then, by combining with technology for decomposing and solving the problem by software means, we will enable Digital Annealer to deal with even larger problems than that capable by only hardware scaling thereby expanding its application domain even further.

3.2 Problem decomposition technology

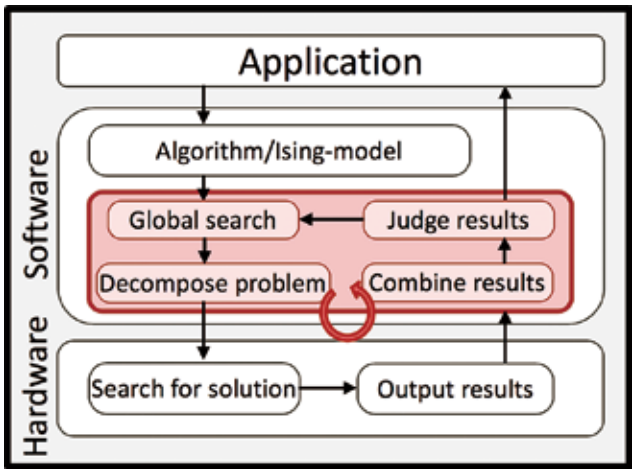
Simply decomposing a large-scale problem into portions that can be input into the system's hardware and optimizing each of these portions does not make for total optimization. This is because mutual relationships exist among these portions such that once one is optimized another is affected. Here, extracting a portion of the problem, fixing the states of the locations not extracted, and optimizing only the extracted location can achieve a partial optimization, but it cannot obtain a sufficient effect if an appropriate location has not been selected.

Against the above background, we developed technology that can process a problem on a scale larger than that possible on hardware alone. Applying this technology to the second-generation Digital Annealer will enable application to problems on a scale of 100,000 bits.

This technology, called the problem decomposition method, begins by determining an initial solution to the entire problem by performing a short-time total search. Next, it extracts a portion of the problem on a scale that can be input to the hardware and searches for a solution to that part using Digital Annealer. It then repeats a flow that returns that result to the total search any number of times while changing the location to be extracted. Finally, it derives a solution for the large-scale problem overall (Figure 4).

An important factor in improving the efficiency of optimizing the entire problem is determining what portions to extract taking the characteristics of the problem into account. For this

Figure 4: Problem decomposition method



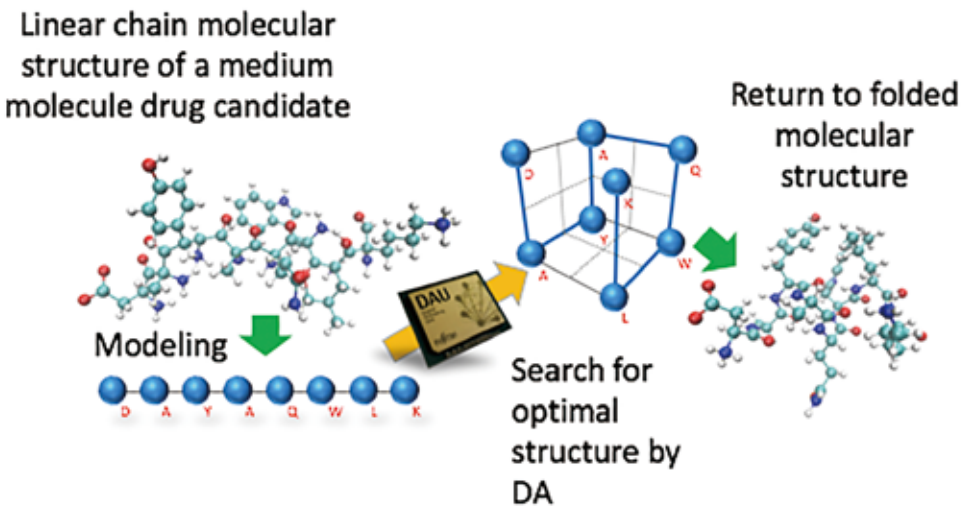
reason, we developed several decomposition methods focusing on relationships within the problem, such as a method that performs extraction centered about elements that easily change within the entire problem and a method that partitions the problem into locations for which inter-element bonding is small. Selecting a decomposition method applicable to the target problem enables solution searching with good efficiency for large-scale problems.

3.3 Application to a stable structure search problem

Focusing on simulation seeking a stable structure of a medium molecule drug candidate, we have confirmed that Digital Annealer using the above problem decomposition technology can be applied to large-scale problems as described below (Figure 5).

In medium molecule drug discovery, a medium molecule drug candidate that connects several to about 50 amino acids in a chain can demonstrate a drug effect by binding strongly with a targeted protein. To this end, the first step is to use Digital Annealer to search for the most stable structure after modeling each amino acid as a point on a lattice based on binding relationships among

Figure 5: Application to a stable structure search problem



those amino acids. The next step is to investigate the binding strength between the amino-acid structure just found and the target protein through docking calculations. Repeating this flow about 1,000 times enables a medium molecule drug candidate with high drug efficacy to be found.

We have demonstrated that applying this problem decomposition technology to the second-generation Digital Annealer can shorten simulation time for a medium molecule drug candidate on a scale of 48 amino acids (30K bits) from several hours by a conventional computer using the same technique for modeling amino acids to several minutes. We expect the application of the developed technology to Digital Annealer to accelerate the development of medium molecule drugs that have been attracting attention as next-generation drugs.

4. Expansion of application fields

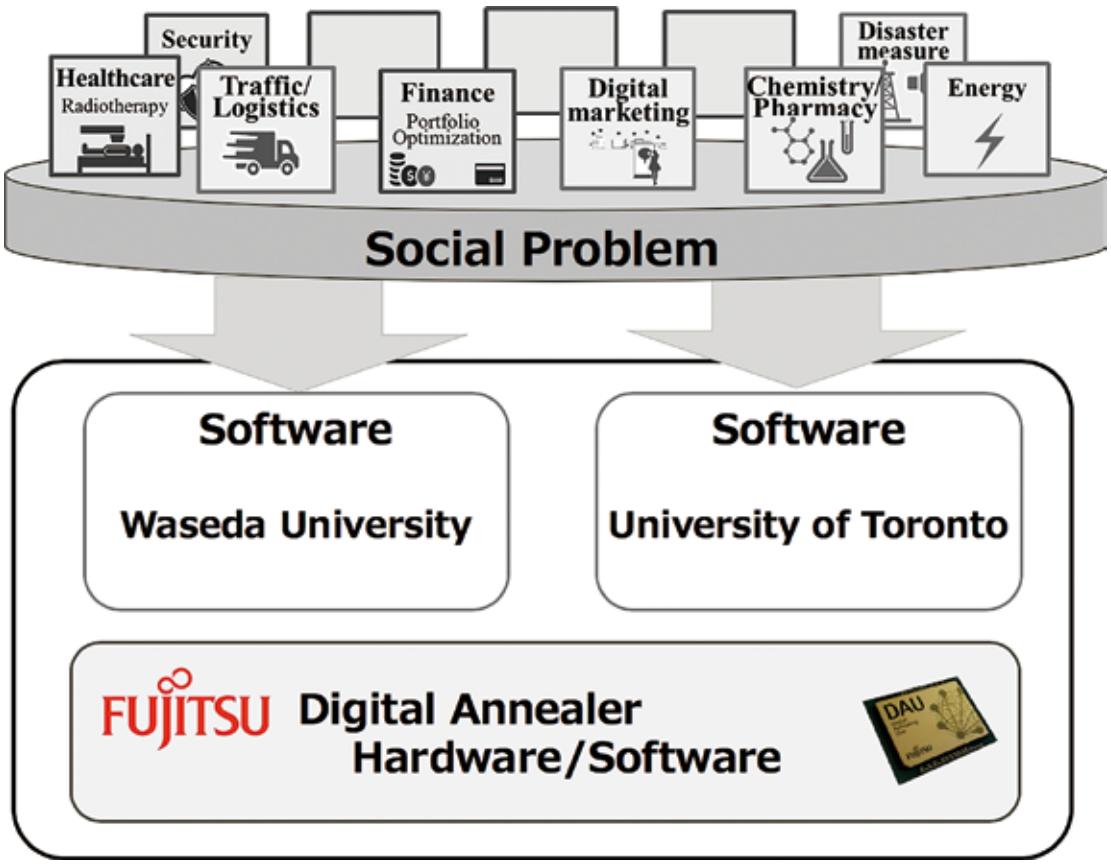
To apply Digital Annealer to combinatorial optimization problems in a variety of real-world fields, it will be necessary to develop software for application to real problems in collaboration with specialists in those fields. In this regard, 1QB Information Technologies Inc. (Headquarters: Vancouver, Canada), a company excelling in the development of quantum computing applications, began collaborative work with Fujitsu in 2017 including the construction of an application development platform. Fujitsu Laboratories, meanwhile, entered into a strategic partnership with the University of Toronto also in 2017 establishing a research center in Toronto. It also concluded a comprehensive collaborative activity agreement with Waseda University for joint research on Digital Annealer in 2018 that included the establishment of a joint-research center (Figure 6). Going forward, Fujitsu plans to incorporate the results obtained from such joint research into Digital Annealer business with the aim of promoting solutions to real-world problems and contributing to social development and economic growth.

5. Conclusion

In this paper, we described the architecture of Digital Annealer, an optimization calculation engine for solving combinatorial optimization problems, and introduced acceleration and scaling technologies. Going forward, we plan to incorporate more acceleration and scaling technologies into Digital Annealer as needed. Furthermore, in addition to improving performance, we intend to expand the range of application fields through joint research with diverse research institutions and contribute to business in various fields.

References
[1] R. Colwell, "The Chip Design Game at the End of Moore's Law," Hot Chips 27, 2015.
[2] K. Fukushima, "On The Front Lines of the Monte Carlo Method—Roll the Dice and Integrate Method," Grant-in-Aid for Scientific Research on Priority Areas "Statistical Mechanical Approach to Probabilistic Information Processing (SMAPIP)" (sponsor), Lectures Providing Easy-to-understand Introductions to New Technologies to Young Researcher and Students "Information Processing by Probabilistic Algorithms" 2003. (in Japanese)
[3] K. Hukushima and K. Nemoto, "Exchange Monte Carlo Method and Application to Spin Glass Simulations," J. Phys. Soc. Jpn., 65, pp. 1604-1611 (1996).

Figure 6: Digital Annealer community



Overview of CMOS Annealing Machines

Masanao Yamaoka
Senior Researcher
Research & Development Group, Hitachi, Ltd.

1. Introduction

As the Internet of Things (IoT) becomes commonplace, it requires more computing capacity. In computers with a von Neumann architecture, the scaling of semiconductor devices has so far supported exponential increases in processing capability, thereby ensuring that it has always been possible to deliver the required performance. However, it is now being said that the scaling of semiconductors is coming to an end, and this will make it difficult to improve the performance of conventional von Neumann type computers. Also, considering the future needs of the IoT era, it will be necessary to implement diverse forms of control in a wide variety of systems used by society. This will require the optimal setting of multiple system control parameters, which will entail processing combinatorial optimization problems at high speed.

One method that has been proposed for efficiently solving combinatorial optimization problems involves using an annealing machine based on the Ising model[1][2][3]. Although annealing machines have been implemented in various different ways, we have proposed a CMOS annealing machine that uses semiconductor circuits to simulate an Ising model[4][5][6]. We built a prototype of this CMOS annealing machine and confirmed that it can efficiently process a type of combinatorial optimization problem called the "maximum cut" problem. We also built a prototype second-generation CMOS annealing machine using FPGAs and were able to confirm not only that it can solve more complex combinatorial optimization problems, but also that even larger-scale problems can be solved by connecting multiple second-generation CMOS annealing machines.

2. Combinatorial optimization problems and annealing machines

Combinatorial optimization problems are problems that involve searching for a solution comprising a set of parameters that maximizes (or minimizes) an evaluation function under a given set of conditions. Such problems are characterized in that the number of candidate solutions grows explosively as the number of parameters to be determined increases. In the future, we can expect social systems to become larger in scale and more interconnected, and the number of parameters to be optimized will tend to increase.

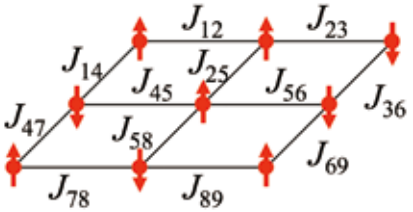
It has been suggested that these combinatorial optimization problems could be solved by using an annealing machine based on the Ising model, which is a statistical mechanics model representing the spin behavior of magnetic bodies. The Ising model is shown in Figure 1. The Ising model consists of "up" and "down" spin states σ_i representing the properties of a magnetic material, an interaction coefficient J_{ij} representing the interaction forces between these two spin states, and an external magnetic field coefficient h_j representing the forces of an externally applied magnetic field. The energy H of the Ising model is expressed by the equation shown in Figure 1. In the Ising model, the spin state is updated to minimize the energy H, eventually yielding the minimal value of H. Combinatorial optimization problems can be solved by using the Ising model as follows. First, the problem is mapped so that the evaluation function of the combinatorial optimization problem corresponds to the energy of the Ising model. Here, the parameters of the optimization problem correspond to the spin values of the Ising model. Next, convergence operations are applied to the Ising model, resulting in a combination of spin states that minimizes its energy. By observing these spin values and mapping their state back to the original optimization problem, it is possible to ascertain the combination of parameters that minimizes the evaluation function, i.e., the solution to the combinatorial optimization problem.

3. CMOS annealing machine

We have proposed a method for simulating an annealing machine in semiconductor CMOS circuits and using it to process combinatorial optimization problems. Since it uses CMOS circuits, it is easy to manufacture, highly scalable, and easy to use.

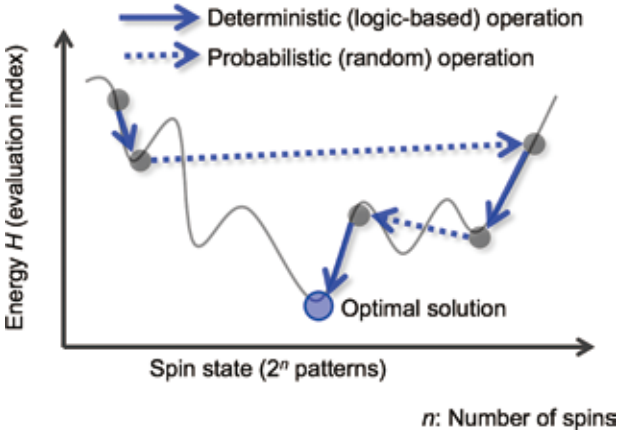
Annealing is an operation that searches for a low-energy state, and is used when searching for the ground state of the Ising model. To perform annealing in CMOS semiconductor devices, it has to be implemented as two operations as shown in Figure 2.

Figure 1: Ising model



$$H = -\sum_{\langle i,j \rangle} J_{ij}\sigma_i\sigma_j - \sum_j h_j\sigma_j$$

Figure 2: CMOS annealing



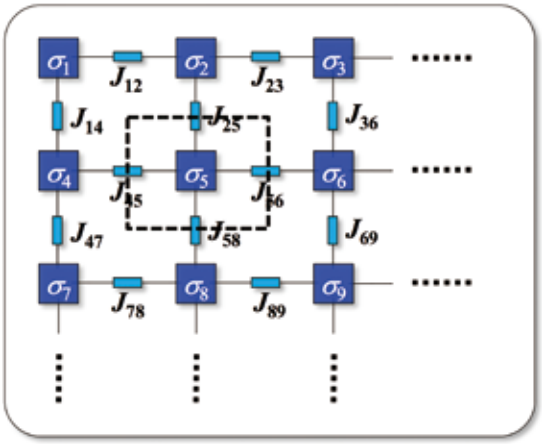
The first operation involves transitioning to a lower-energy state in the energy landscape by a deterministic action as indicated by the solid arrow in Figure 2. With deterministic behavior alone, the algorithm is liable to become trapped in localized energy valleys and will be unable to find other low-energy states. Therefore, in order to escape from these local solutions, the energy state is randomly perturbed by probabilistic operations to search for the lowest possible energy state. The process of searching for a low-energy state by combining these two operations is called CMOS annealing. In CMOS annealing, deterministic operations are performed by modeling interactions between spin states in digital circuits, and the probabilistic operations are performed based on random numbers.

Since CMOS annealing relies on random numbers, it may not always find the optimal solution. However, when this computing technology is used for the optimization of real social systems, it is considered to be acceptable even if it does not always find the absolute optimum value. For example, when searching for traffic routes, a solution can be regarded as acceptable from the viewpoint of system optimization even if it delivers routes that have slightly higher values than the best possible solution. It could therefore be argued that this CMOS annealing technology is geared more towards practicality than strict academic precision.

In the Ising model, the spin states have to be stored as binary values, and thus semiconductor circuits are used to keep them in SRAM. The SRAM also stores the interaction coefficients representing the strength of spin interactions, and the external magnetic field coefficients representing the strength of the external magnetic field. Furthermore, the effects of interactions that update the spin values are simulated by digital circuit operations.

Figure 3 shows the system configuration for implementing CMOS annealing. In this figure, σ_n represents a spin, which is stored as a value of +1 or –1, and J_{ij} represents an interaction between spins. The parts surrounded by the dotted line in this figure represent a single spin interaction processing circuit. This not only stores the actual spin information, but also includes circuits for updating the spin state using the spin effects connected with this spin. CMOS annealing is performed by updating the spin states in these spin circuits. This updating of spin states can be performed simultaneously in parallel for spins that are not connected. For example, in the configuration shown in Figure 3, spins σ_1, σ_3, σ_5, σ_7 and σ_9 are not connected to one another, and can therefore be updated simultaneously. Similarly, spins σ_2, σ_4, σ_6 and σ_8 are also not connected to one another, and can thus be updated simultaneously. In this way, it is possible to update half the total spin states simultaneously in a structure having the (spin connection) topology shown in Figure 3. That is, with this

Figure 3: Configuration of CMOS annealing machine



configuration, any number of spin states can be updated in just two cycles. This means it is possible to suppress increases in the time required for processing even when the scale of the device is increased.

The probabilistic operation of the CMOS annealing operation in Figure 2 introduces random number sequences into the spin circuits. By evaluating these random number sequences, the spin values are stochastically flipped. This causes random transitions to unrelated states as shown by the dotted lines in Figure 2[7][8]. By performing CMOS annealing in combination with the interaction of spin states and probabilistic state transition actions, it is possible to find as many low-energy states of the Ising model as possible.

4. Prototype CMOS annealing machine

To demonstrate the operation of the proposed CMOS annealing machine, we used 65 nm CMOS process technology to fabricate an Ising chip to reproduce the CMOS annealing operations. A photograph of this chip is shown in Figure 4(a). It contains 20,000 spin simulator circuits in a chip measuring 3 mm × 4 mm. Each spin simulator circuit measures 11.27 × 23.94 = 270 μm^2. The interface circuit for reading and writing the spin states and interaction coefficients from outside operates at 100 MHz, which is the same as the rate of the interaction operations that update the spin values.

This Ising chip incorporates a three-dimensional Ising model consisting of two interconnected layers of two-dimensional lattice Ising models. The three-dimensional Ising model is embedded in a two-dimensional memory structure. Semiconductor chips use two-dimensional structures to achieve a high integration density, and our Ising chip achieves a high integration density in the same way, allowing it to simulate a large number of spin states. Figure 4(b) shows a prototype Ising computing node with two Ising chips. This prototype can solve optimization problems supplied to it from a PC or a server via a LAN.

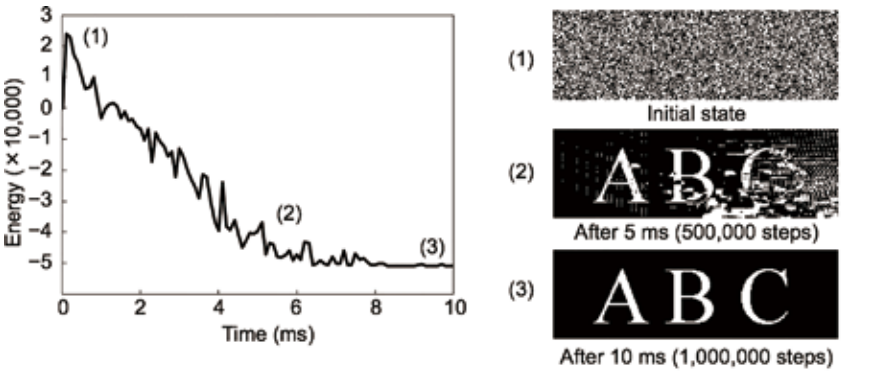
Figure 5 shows the results of using the Ising chip to solve a maximum cut problem (a kind of NP-complete combinatorial optimization problem). Figure 5(a) shows how the energy of the Ising model changes when solving this problem. During CMOS annealing, it can be seen that the energy decreases with time, and finally reaches the minimum energy after 10 ms. The changes of spin state that occur when solving this problem are illustrated by the black and white images in Figure 5(b). Here, white and black points represent "up" and "down" spins, respectively. The problem being solved in this example was chosen so that the letters "ABC" would appear clearly when the spin states corresponding to the optimum solution had been found. As the changes of spin state in this picture clearly show, the spin states start off in a random initial state with an irregular arrangement of white and black points. After 5 ms, the energy of the Ising model has decreased, and the characters ABC have started to emerge from

Figure 4: First generation prototype

(a) Prototype chip

(b) Prototype Ising computing node

Figure 5: First generation prototype measurement results



(a) Variation of Ising model energy when solving maximum cut problems

(b) Variation of Ising model spin states when solving maximum cut problems

the noise. However, the inclusion of noise shows that this state is only a local solution. When the CMOS annealing operations are continued, the energy falls further still. After 10 ms, the ABC characters can clearly be seen without any noise. This is the minimum energy state, showing that the optimum solution to the maximum cut problem has been found. Although it was possible to obtain the optimum solution in this example, it is not always possible to obtain the optimum solution due the probabilistic nature of CMOS annealing as described above. However, we have confirmed that this operation results in a reduction of energy and is capable of finding as good a solution as possible to combinatorial optimization problems.

As a second-generation prototype, we also fabricated a CMOS annealing machine from FPGAs. A photograph of this prototype is shown in Figure 6(a). Since this prototype uses FPGAs, it allows various different Ising model topologies and interaction coefficients to be tried out. To take advantage of this flexibility, we developed an embedding algorithm to embed the Ising model in the hardware topology[9]. With this algorithm, it is possible to run real-world combinatorial optimization problems on a CMOS annealing machine.

Another major advantage of CMOS annealing machines is that they can easily be scaled up by connecting multiple chips together. This is because the calculations are performed by digital circuits, so by exchanging digital signals between the chips, it is possible to perform the same operations as would be performed in a single chip. Since the spin states are sparsely connected in the CMOS annealing machine, another advantage is that the information about spins in one chip can be easily sent to another connected chip. To confirm this scalability, we constructed a large-scale 100 kbit machine by connecting together two second-generation prototypes. With this architecture, we were able to solve huge problems 25 times larger than could be solved by the second-generation hardware alone. This means it is possible to handle social problems that will become more prominent in the future (Figure 6(b)).

5. Conclusion

We have built a CMOS annealing machine based on CMOS semiconductor circuits. Our first-generation prototype can simulate about 20,000 spin states. In the future, it will be possible to reproduce even larger Ising models by making use of finer semiconductor processing. Furthermore, we have shown that spin interactions can be calculated using digital values. This means that further increases of scale can easily be achieved by interconnecting multiple chips. Using a second-generation prototype, we confirmed that this multiple chip configuration works properly. From the viewpoint of ease of use and scalability, it can be said that this semiconductor-based approach is a significant engineering achievement. We have confirmed that our prototype CMOS annealing machine is capable of solving actual maximum cut combinatorial optimization problems. It is known that maximum cut problems can be transformed mathematically into other combinatorial optimization problems, so we believe that this architecture can be used in the optimization of real-world systems.

References
[1] W. Johnson et al., "Quantum annealing with manufactured spins," Nature 473, pp. 194–198, 12nd May 2011.
[2] T. Inagaki et al., "A coherent Ising machine for 2000-node optimization problems," Science 20, Oct 2016, DOI: 10.1126/science.aah4242.
[3] P.L. McMahon et al., "A fully-programmable 100-spin coherent Ising machine with all-to-all connections," Science 20, Oct 2016, DOI 10.1126/science.aah5178.
[4] C. Yoshimura et al., "Spatial computing architecture using randomness of memory cell stability under voltage control", 21st European Conference on Circuit Theory and Design, September 2013.
[5] M. Yamaoka et al., "20k-spin Ising Chip for Combinational Optimization Problem with CMOS Annealing," ISSCC 2015 digest of technical papers, pp. 432–433, Feb., 2015.
[6] M. Yamaoka et al., "A 20k-Spin Ising Chip to Solve Combinatorial Optimization Problems With CMOS Annealing," IEEE J. Solid-State Circuits, vol. 51, no. 1, pp. 303–309, Jan. 2016.
[7] M. Hayashi et al., "An Accelerator Chip for Ground-State Searches of the Ising Model with Asynchronous Random Pulse Distribution," 2015 Third International Symposium on Computing and Networking (CANDAR), pp. 542–546, Feb. 2015.
[8] M. Hayashi et al., "Accelerator Chip for Ground-state Searches of Ising Model with Asynchronous Random Pulse Distribution," International Journal of Networking and Computing, vol. 6, no. 2, pp. 195–211, July 2016.
[9] T. Okuyama et al., "Computing architecture to perform approximated simulated annealing for Ising models," International Conference on Rebooting Computing, Oct. 2016.

Figure 6: Second generation FPGA prototype

(a) 4 kbit machine (b) A 100 kbit machine made by connecting 25 FPGAs

= A Serial Introduction Part 2 = Winners of ITU-AJ Encouragement Awards 2018

In May every year, The ITU Association of Japan (ITU-AJ) proudly presents ITU-AJ Encouragement Awards to people who have made outstanding contributions in the field of international standardization and have helped in the ongoing development of ICT.
These Awards are also an embodiment of our sincere desire to encourage further contributions from these individuals in the future.
If you happen to run into these winners at another meeting in the future, please say hello to them.
But first, as part of the introductory series of Award Winners, allow us to introduce some of those remarkable winners.

Toru Uchino
NTT DOCOMO, INC.
tooru.uchino.fv@nttdocomo.com https://www.nttdocomo.co.jp/english/
Fields of activity: 3GPP LTE-Advanced and 5G standardization

3GPP standardization activity on LTE-Advanced and the 5G higher layer protocol

I am extremely honored to receive the ITU-AJ Encouragement Award, and would like to thank the ITU Association of Japan and all those who supported my nomination and selection.

When I first joined NTT DOCOMO in 2009, I worked on development of the LTE commercial base station which was launched in 2010. I then began attending 3GPP RAN2 meetings in 2011 and contributed to Carrier Aggregation (CA) specifications to boost data rates by aggregating multiple carriers, Dual Connectivity (DC) to enhance data rates by enabling terminals to communicate with multiple base station, and IoT terminals. For two years from December 2013 to December 2015, I was privileged to serve as Work Item rapporteur for CA and DC WIs, with responsibility for coordinating work item schedules and discussions.

Many stakeholders come together from diverse backgrounds—private companies, common carriers, vendors, and research institutions—to create standard specifications in 3GPP meetings. So in order to reach a consensus when drafting an agreement, it's essential that we consider not only the technical aspects but the background of the companies or institutions making the proposals. Needless to say, it is quite a challenge to organize and compile all of the information needed to conduct constructive discussions when literally hundreds of contributions are submitted from such a diverse membership for every CA and DC work item under discussion. As WI rapporteur, my job is to facilitate the discussions so things go smoothly in order to complete the specification work on schedule.

More specifically, my job involved sorting out from among the companies' many proposals those ideas and contributions that were critically important for the system, and negotiating to keep the good ideas while excluding the nonessential content. Eventually, with much support from my colleagues, we successfully completed the specification on schedule.

3GPP has now completed the official standalone 5G specification, which opens the way to discussions of 5G enhancements. As more emerging companies and stakeholders join the discussion, this will present even greater challenges. But based on my years of experience working for the 3GPP, I am fully committed to further development of 5G system specifications which will usher in even better user experience and more efficient new radio systems.

Nobuo Okabe
SHARP Corporation (Retired)
JH1LRO@ybb.ne.jp
Fields of activity: Expert of JICA (Japan International Cooperation Agency)

Installation of Digital Terrestrial Television Broadcasting (DTTB) and Emergency Warning Broadcasting System (EWBS) in Peru

I am extremely honored to receive the ITU-AJ Encouragement Award, and thank everyone involved in my nomination and selection.

I served two years as a JICA expert charged with helping disseminate digital terrestrial TV broadcasting (DTTB) and the emergency warning broadcasting system (EWBS) in Peru. Having decided to adopt Japan's ISDB-T international standard, Peru has already rolled out digital broadcasting in six major cities.

Peru's Institute of Radio and Television (IRTP) has 192 television broadcasting stations spread across the country, and government's Ministry of Transport and Communications (MTC) is promoting nationwide digitalization in line with the ministry's master plan. But in promoting the rollout of digital TV to rural areas and the rest of the country, there hasn't been enough effort to educate the citizenry about the upcoming analog "blackout" beginning in 2020 or the fact that current analog TV sets will no longer be supported. Capitalizing on my experience rolling out digital TV in Japan, my mission was to collaborate with MTC staff in charting a deployment roadmap that is tailored to Peru's unique circumstances.

In 2016, six digital stations and eight tide level gages were set up as a trial EWBS system for Peru, and continuous broadcasting trials have been conducted to verify that the system works exactly as it is supposed to. The EWBS system has attracted enormous interest

among other South and Central American countries that are also subject to life-threatening natural disasters.

Although my mission in Peru has come to an end, I still follow up with inquires that come in from time to time from Japan's Ministry of Internal Affairs and Communications (MIC) and other relevant agencies.

We are making an effort to get the EWBS system widely deployed in as many Central and South American countries as possible, because it really has the ability to save a lot of lives when natural disasters strike.

Masaaki Obara

KDDI Corporation
ms-obara@kddi.com http://www.kddi.com/english/
Fields of activity: 3GPP RAN

Efficient utilization of spectrum via 3GPP standardization activities

I am honored to receive the prestigious ITU-AJ Encouragement Award, and would like to thank everyone who supported my nomination and selection.

It is well-known that mobile data traffic has grown prodigiously averaging 30 to 40% a year in Japan. Efficient utilization of spectrum is a critical factor in accommodating this rapid growth. There are several candidates for improving efficiency in a 3GPP context, and my work has focused on standardizing *Carrier Aggregation*, or CA.

CA is achieved by aggregating spectra, or component carriers (CC). So for example, 800MHz + 2GHz is referred to as 2CC CA, 800MHz + 1.7GHz + 2.1GHz is designated 3CC CA, and so on. One can see that the peak data rate is significantly improved by CA. Essentially, the required time to transmit and receive data is slashed compared with using a single spectrum. In other words, by shortening the time for data communication, this frees up radio resources that can be used by other users, so CA greatly improves the efficiency of spectrum utilization.

Having analyzed and demonstrated these advantages of CA, KDDI proceeded to develop a detailed road map for CA commercialization based on 3GPP standardization. I am convinced that CA is critically important for improving the user experience. I was in charge of standardization during this time frame, so I put together a viable work plan for achieving the CA commercialization roadmap. I proposed new work items to be addressed by 3GPP TSG-RAN in my capacity as rapporteur and received approval to commence technical discussions at the end of 2011. I also coordinated technical discussions in 3GPP RAN-WG4 while managing the commercialization schedule. Although KDDI's proposals were not universally accepted, they were clearly necessary for drafting a CA specification that would enhance user experience. These efforts proved successful thanks to the many stakeholders who supported my standardization efforts. Finally, in the summer of 2014, KDDI was Japan's first operator to commercially launch CA.

Spectrum efficiency has been markedly enhanced by CA, but mobile data traffic continues to expand. KDDI is committed to optimizing the user experience, and will continue to play a prominent role in 5G standardization and technologies now emerging.

Ataru Kobayashi

NEC Corporation
a-kobayashi@df.jp.nec.com
https://www.nec.com/en/global/solutions/biometrics/index.html
Fields of activity: Safety / ITU-D SG2

Safe and Smart Society

It is a great honor to receive this award. NEC has a track record in development and worldwide deployment of face recognition technologies; last year, NEC's TCI Division (now Safer City Solutions Division) has also received the ITU-AJ Encouragement Award. Beginning with the Regional Preparatory Meeting for WTDC-2017 for Asia and the Pacific, as well as during the WTDC-2017, and currently as part of the ITU-D Study Group on Smart Society Q1/2, I have continued carrying out initiatives aimed at communicating the importance of and sharing relevant case studies on "safety and security of society," in which face recognition and other biometric authentication technologies play a significant role, with officials from developing countries.

Major risks are inevitable when the creation of smart societies is hastily pursued. Societies become vulnerable in the absence of safety measures that are commensurate with the investment in digital technology. In regard to safety measures, studies on cybersecurity (Q3), disaster recovery (Q5), and e-Health (Q2) are already being undertaken within ITU-D Study Group 2. Thus, I would like to delve into the ICT needed for (personal) safety under smart society (Q1).

No matter how convenient and efficient cities and societies become, safety will always be an important component of people's Quality of Life (QoL). ICT systems, such as surveillance cameras and face recognition systems, play an important role in ensuring public safety in cities, train stations, event venues, and other public places. Likewise, ICT is also essential in digital government, which enables digitalization of administrative procedures and equal access to safe public services for all citizens. Another area that requires ICT is smart transportation, which enables congestion- and accident-free transportation, as well as the safe use of public transportation by women and children.

Along with proposing relevant case studies in Japan and overseas, I would like to convey the importance of safety and security in smart societies to officials of developing countries.

New Breeze
平成三十一年一月十日発行（年四回一、四、七、十月の十日発行）第三十一巻第一号（通巻百二十一号）

The ITU Association of Japan

定価　一冊　一、六二〇円（本体価格　一、五〇〇円、消費税　一二〇円）　年間購読料　六、四八〇円（本体価格　六、〇〇〇円、消費税　四八〇円）