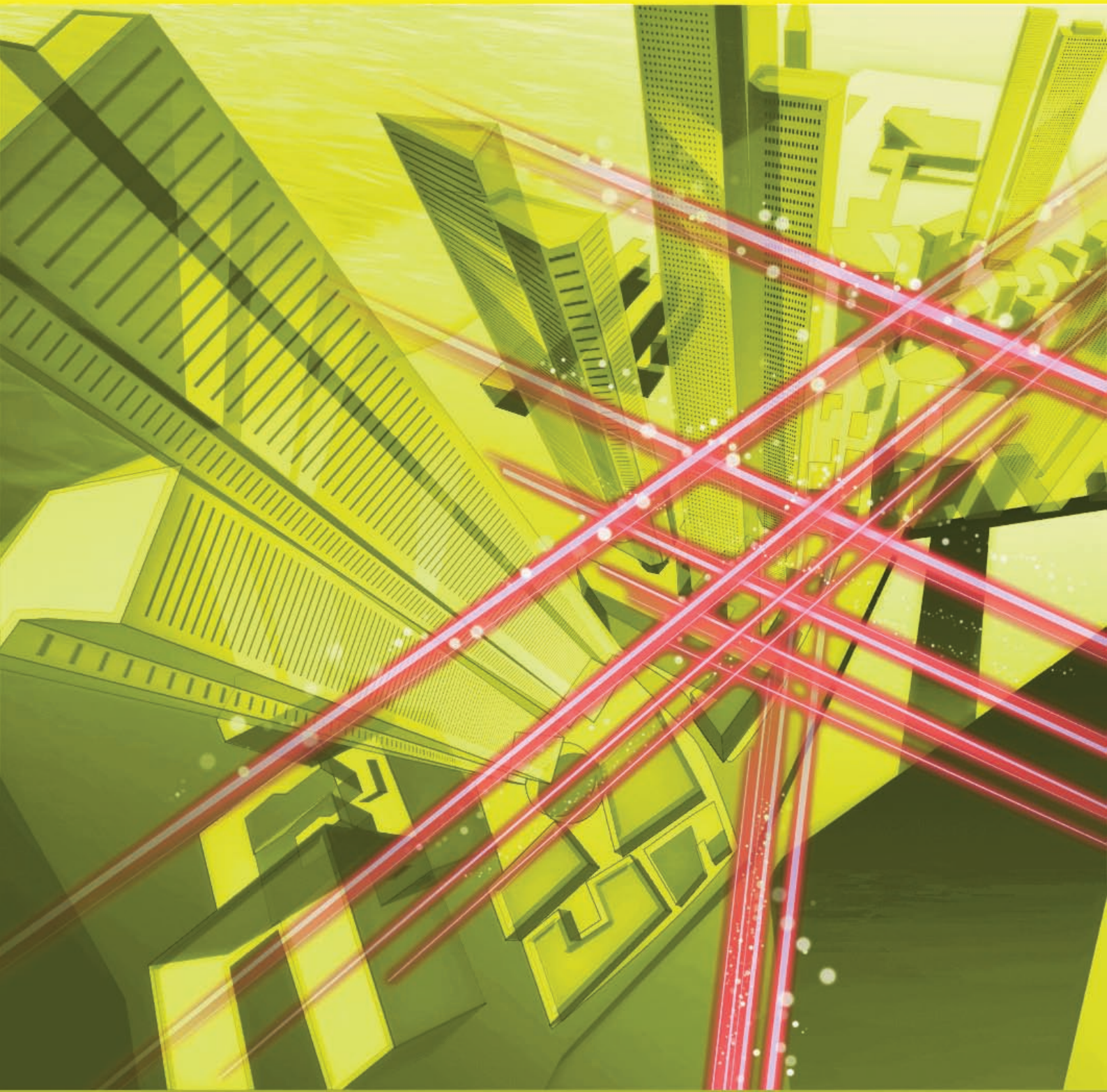
NTT Technical Review

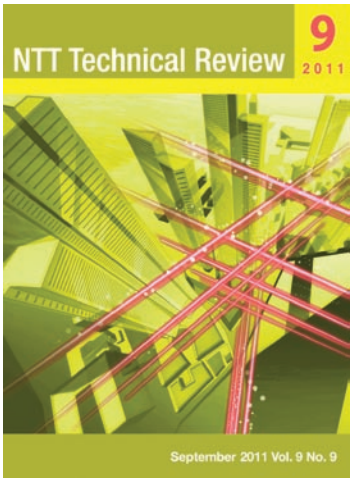
9
2011



September 2011 Vol. 9 No. 9

NTT Technical Review

September 2011 Vol. 9 No. 9



Mission of the ICT Design Center

Yoichi Kato†*, Yoko Asano, and Takehiko Ohno*

Abstract

This article reviews human-centered design and introduces the activities of the ICT Design Center (IDeC) of NTT Cyber Solutions Laboratories, which is striving to create user-friendly information and communications technology (ICT) services by utilizing various techniques of human-centered design and cognitive psychology.

1. Introduction

It is great to produce easy-to-read manuals that guide users without confusing them, applications that provide an enjoyable experience, and operating manuals that significantly minimize the possibility of human errors. How can we achieve these goals?

One of the criteria used for evaluating products and services is the quality of experience (QoE) [1]. Users have various feelings when they use products and services such as being happy or bored. When the feeling is positive, the QoE of the product or service is considered to be high. Two products with the same set of functions may have quite different sales volumes because of differences in their QoEs.

The QoE of a product or service is determined not only by the experience of using it but also by the purchasing process, packaging, and manual. In particular, user experience from opening a product's package to its first use (called the out-of-box experience) affects the QoE significantly. Making this experience smooth and pleasant increases the QoE and decreases user support costs [2].

Usability is the concept of how easy-to-use and user-friendly a product or service is. Nielsen, one of the masters of usability studies, defines the elements of usability as learnability, efficiency, memorability, errors, and satisfaction [3]. Steps needed to improve the QoE and usability include analyzing users' thoughts and behaviors, identifying problems and their causes (evaluation), and consequently improving the design (improvement).

† Broadband Media Business, NTT IT
Naka-ku, 231-0032 Japan

Network maintenance technicians use well-structured operation manuals that include a lot of know-how gleaned from a long history of consideration. The manuals help to reduce human error. To reduce the error even more, we can utilize knowledge discerned through cognitive science. For example, by measuring the cognitive load (number of items that a technician must take care of at the same time) in each step of the operation, we can identify operations that require too much attention. In this case, the two steps of evaluation and improvement, are important.

Human-centered design is a design philosophy focusing on human thinking and behavior [4], [5]. This concept can be applied to improve various business procedures as well as the usability and QoE of products and services.

The ICT Design Center (IDeC) of NTT Cyber Solutions Laboratories is striving to create user-friendly information and communications technology (ICT) services by utilizing various techniques of human-centered design and cognitive psychology. This article reviews human-centered design and briefly introduces IDeC's activities. More details of specific activities are given in the other Feature Articles on this theme.

2. Human-centered design

It is essential to know human characteristics in order to use the human-centered design process (**Table 1**). For example, knowing the user's behavior and the underlying psychology in depth is important in order to respond appropriately when a user claims that a service or product is hard to use.

The general procedure of human-centered design is

Table 1. Human characteristics.

Human attributes	Explanation	Examples of problems in human interface
Perception	Sight, hearing, touch, etc.	Display is too small, bad audio quality, slippery knobs.
Cognition	Comprehending things, e.g., understanding that clicking a button on a web page loads and displays another page	A button on a web page may not be well recognized as a button if the design is done poorly.
Body	The structure and size of the human body, e.g., finger size	A button on a control panel is hard to press if it is too small compared with the size of the finger tip.
Emotion	Emotion from the experience of using a product or service: fun to use or not	The design of the product is unfriendly or unattractive.

shown in **Fig. 1**. The first step is to identify the problems in existing products and services or in early-phase prototypes. For this purpose, user behavior observations and interviews targeting usability are commonly performed. Once the problems have been identified, the designers think of solutions and a prototype is made. Next, the prototype is evaluated and it is determined whether or not the problems have been solved. If the results are unsatisfactory, the designers must return to the solution-creation step and make a new prototype (repeating the design cycle).

The choice of evaluation methods used in the problem-identification and prototype-evaluation phases is important. In human-centered design, it is fundamental to study and analyze user behaviors and the thoughts behind them precisely.

The human-centered design methodology has been developed most actively in the design areas of home appliances and office equipment. It can be applied to various work process improvements. For example, replacing "existing products and services" in Fig. 1 with "network troubleshooting procedure" yields the following process: first, observe a network technician trying to fix a problem with an existing operation manual; it is then possible to improve the identification of problems and points in the procedure, improve the manual, and improve the manual's evaluation. The important point is to trace the technician's thoughts step by step in order to identify what caused the problem.

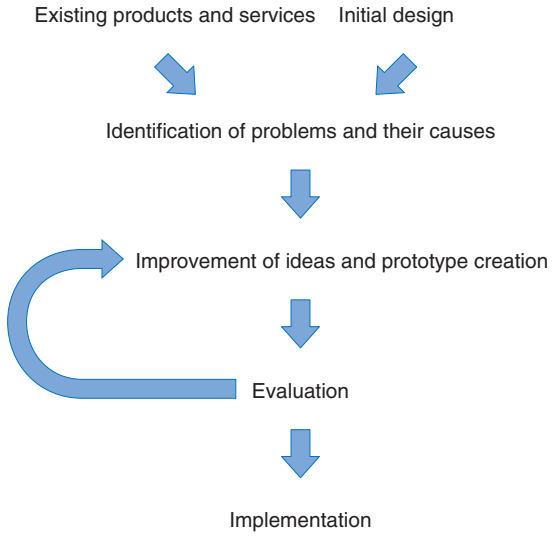


Fig. 1. Procedure of human-centered design.

3. Methods for studying and analyzing human behaviors and thoughts

Many methods have been proposed for studying and analyzing the behaviors and thoughts of people using products and services. It is important to choose the one best suited to the purpose of the analysis [6], [7]. This section briefly introduces some of the methods. Note that the users who participate in the study and analysis are called *subjects* here.

3.1 Research and analysis methods for problem-identification phase

Imagine that you have a vague feeling that the QoE or usability of a product or service needs to be improved (perhaps on the basis of user feedback that it is hard to use), but you do not know what the real problems are or where they lie. In such cases, you first need to identify the real problems and their fundamental causes. This is called the problem-identification phase.

(1) Observation

Observation is a powerful tool for finding the problems and causes of poor usability in products and services. If possible, you can record such scenes on video and analyze them in detail afterwards to get

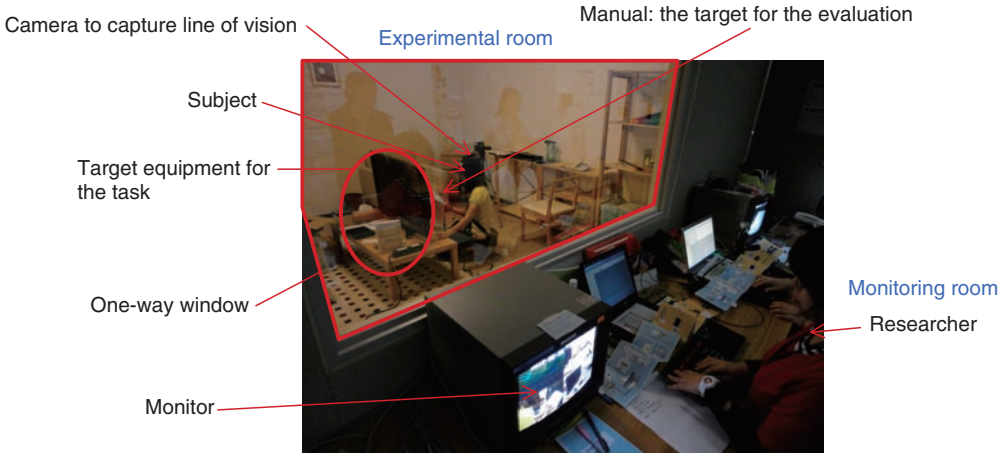


Fig. 2. Configuration of usability lab.

better results. To analyze a subject's thoughts directly, we sometimes ask the subject to say what he or she is thinking at each moment (*speak aloud* method). Observation is done either at an actual place of use or in a usability lab. An example of a usability lab is shown in **Fig. 2**; here, the task was to evaluate the manual for setting up an IPTV (Internet protocol television). Observational methods allow us to find problems that are hidden in the subject's unconscious behavior.

(2) Interviews and questionnaires

Interviews and questionnaires are commonly used in usability testing to identify problems and their causes. It is easy to find superficial problems by a simple analysis of the results. However, to find fundamental and hidden causes of the problems, it is necessary to analyze in depth the interview scripts and the free descriptions submitted as questionnaire results.

For example, using the grounded theory approach, we first break scripts down into sentences and words and then find the relationship among them. Thus, we can comprehend the transitions in the subjects' thoughts at a deep level and find the fundamental causes of the problems.

(3) Evaluation by usability specialists

Usability specialists perform a heuristic evaluation using a checklist that consists of known and common causes of misunderstanding, misdirection, and misoperation. This method is mainly used in the early phase of prototyping to identify superficial problems with usability.

3.2 Research and analysis methods for evaluating prototypes

Once the problems have been identified and you come up with a solution, you then need to evaluate its effectiveness. When you have multiple solution candidates, you need to measure the effectiveness of each solution to choose the best one. In these cases, quantitative evaluation methods are used.

(1) Subjective evaluation

Subjects grade the usability and performance using multiple levels (e.g., five) to grade characteristics such as response speed.

(2) Objective evaluation

Subjects perform tasks using an improved target product or service. By measuring the task's success rate and the time taken to complete the task, we can quantitatively compare the effectiveness of different improvements. The quantitative data are processed by using statistical methods. For example, when we performed subjective tests on two interface design candidates, one candidate had a slightly higher average score than the other. To determine whether the former candidate is really better, we can use the t-test (a commonly used statistical method) to take into account the number of subjects and the dispersion of the data.

4. IDeC activities

IDeC is studying the methodologies needed to implement the human-centered design concept and improve the QoE of the products and services of the NTT Group and to improve the group's work

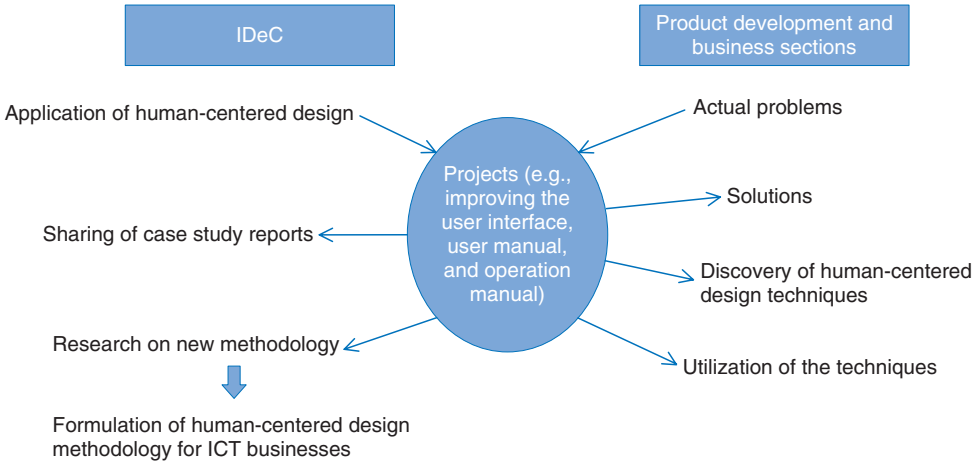


Fig. 3. Activities of IDeC.

processes (**Fig. 3**). Its main activities are to provide solutions and support for common problems in the NTT Group and to provide consultation for specific problems in work places. For the former purpose, it studies common problems in the diverse areas covered by NTT and provides solutions. Some examples of such solutions are popularization through the use of universal design for web applications (web accessibility) and a tool for checking this and related consultation and producing design guidelines for various human-machine interfaces [9]. IDeC provides consultation to resolve specific QoE problems, improve usability, and reduce human error. For example, one project aimed to improve the user manual for home gateway replacement, as described in the third article in this set of Feature Articles [10].

5. Concluding remarks

The Feature Articles on this first theme introduce the concept of human-centered design and the direction of NTT's research and describes four examples of the application of human-centered design. The authors hope that these examples will let readers better comprehend the human-centered design concept with a view to applying it to their own ongoing or future development projects.

The ultimate goal of IDeC is to reach a state where the human-centered design process and techniques are commonly used in every region of the ICT industry. In 1999, an international standard for human-centered design was established [11]. Unfortunately, the current human-centered design processes and techniques are not very easy for beginners to utilize effectively and get desired results. In particular, there are few examples of their use in ICT.

IDeC continues to contribute by developing human-centered design methodologies suitable for ICT businesses and by expanding their deployment in the business sectors to support QoE enhancement activities.

References

[1] "Quality Criterion that User Feels—An Example of Developing IPTV Service," Edited by NTT Cyber Solution Laboratory, Tokyo Electronic Publications Service, 2009 (in Japanese).
[2] M. Nakatani, Y. Katagiri, and M. Miyamoto, "Research on the Structure of the Package for Easy Navigation: Analysis of Eye Movement and the Location of the Documents," 2008, IEICE HIP, Vol. 107, No. 553, pp. 37–42 (in Japanese).
[3] J. Nielson, "Usability Engineering," Morgan Kaufman, 1993.
[4] T. Tarumoto, "Usability Engineering," Ohmsha, 2005 (in Japanese).
[5] T. Kelley and J. Littman, "The Art of Innovation," Currency/Doubleday, 2001.
[6] Y. Kato, S. Yonemura, M. Nakatani, and G. Irie, "Human Characteristics Evaluation and the Applications," Signal Processing, Vol. 14, pp. 177–188, 2010 (in Japanese).
[7] "Human Factors Guide," Edited by T. Fukuda's Laboratory, Scientist, 2006 (in Japanese).
[8] Y. Kinoshita, "Modified Grounded Approach," Kobundo, 2003 (in Japanese).
[9] M. Watanabe, D. Asai, H. Saito, and K. Morita, "Web Accessibility Evaluation Technology," NTT Technical Review, Vol. 9, No. 9, 2011. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa2.html
[10] Y. Asano, S. Yonemura, A. Hayashi, and R. Hashimoto, "ICT Service Design for Senior Citizens Based on Aging Characteristics," NTT Technical Review, Vol. 9, No. 9, 2011. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa3.html
[11] ISO 13407:1999. http://www.iso.org/iso/catalogue_detail.htm?csnumber=21197

Yoichi Kato
Vice President and General Manager, Broadband Media Business, NTT IT.

He received the B.S. and M.S. degrees in electrical engineering from Chiba University and the Ph.D. degree from the University of Tokyo in 1982, 1984, and 1994, respectively. Since joining Nippon Telegraph and Telephone Public Corporation (now NTT) in 1984, he has been working in R&D of videoconferencing systems. In the late 1980s, he actively contributed to ITU-T SG15 in making the H.261 video compression standard. In 2001, he started a web conference business called MeetingPlaza at NTT IT and led the business until 2007. From 2007 to 2011, he was the project director of the Human Interaction Project in NTT Cyber Solutions Laboratories, where he led research on human-centered design, video applications, IPTV applications, and digital signage. He currently leads the business of various video processing applications at NTT IT. His work "Exploring Edo", a computer graphics (CG) simulation of Edo on a shared three-dimensional virtual world platform called InterSpace, received a prize at Dream Centenary CG Grand Prix '99 in Aizu, Japan. He is a member of IEEE, the Institute of Electronics, Information and Communication Engineers (IEICE), and the Institute of Image Information and Television Engineers.

Yoko Asano
Senior Research Engineer, Supervisor, Human Interaction Project, NTT Cyber Solutions Laboratories.

She received the B.E. degree in administration engineering from Keio University, Kanagawa, in 1988 and joined NTT Human Interface Laboratories the same year. She moved to NTT Cyber Solutions Laboratories in 1999. Since then, she has been conducting research on human interfaces. She is a member of the Human Interface Society, the Japan Ergonomics Society, and IEICE.

Takehiko Ohno
Senior Research Engineer, Supervisor, Human Interaction Project, NTT Cyber Solutions Laboratories.

He received the B.Sc. and M.Sc. degrees from Tokyo Institute of Technology, in 1992 and 1994, respectively. He joined NTT Basic Research Laboratories in 1994 and studied cognitive science and human-computer interaction. He has been researching human-computer interaction, human-centered system design, user experience design, usability, gaze tracking technology and its applications, cognitive modeling, information appliances, and computer-mediated communication. He is a member of the Association for Computing Machinery, the Information Processing Society of Japan, the Japan Cognitive Science Society, and IEICE.

Web Accessibility Evaluation Technology

Masahiro Watanabe[†], *Daisuke Asai, Harumi Saito, and Keiji Morita*

Abstract

This article introduces the concept of web accessibility and its associated problems. To identify these problems and correct them easily, we are studying evaluation techniques that judge whether a web design takes accessibility into consideration.

1. Introduction

Japan is becoming an aged society and more and more elderly people are now using the Internet. Moreover, a huge number of people are using personal computers and the Internet, including disabled people. Therefore, it has become increasingly important that everyone can use web content to acquire information, regardless of age or disability. This characteristic is called web accessibility.

To reveal the characteristics of web content, let us compare web content and newspapers. With a newspaper, people who feel that the text and photographs are too small may use a magnifying glass to enlarge them. However, totally blind people cannot read the text in a newspaper and need someone else to read it for them. With web content, on the other hand, it is impossible to obtain information without using some sort of information and communications technology (ICT) such as a web browser on an electronic device. Moreover, people accessing web content can use their own preferred device and browser, and the range that must be supported is quite large.

Blind people can use screen-reading software that utilizes a synthesized voice to read out web content, as shown in **Fig. 1**, and obtain information for themselves without relying on other people. This advantage is a huge feature of web content. In addition, information in the web content can be converted into various presentation formats besides voice. Content can also be displayed on mobile phones and can be converted into braille for presentation on braille devices. Text can be resized or displayed in a high-contrast mode (reverse video) for people who find screens too bright. People who have trouble using a mouse can use input methods that have been tailored for them.

In this way, one web page can be accessed from various different types of devices. An important concept is that web content can be converted into the optimal form for each person using it and that it can be changed. With a newspaper, one would probably have to enlarge the text and make a special issue intended for elderly people, in the same way that some books are available in a large-print edition. However, with a web design intended for elderly people, it is not necessary to enlarge the text beforehand; it is enough to have a web design that allows text to be resized without causing problems.

It should be noted, however, that this conversion needs to be done skillfully; otherwise, problems related to web accessibility can occur. Some specific examples are listed in **Table 1**. Various different scenarios can be considered for the use of web content, such as information being converted into voice, text being displayed, and text being enlarged and displayed. In each of these cases, problems occur, as indicated by these examples. In addition, since a completely blind person cannot use a mouse to control an ICT device because he or she cannot see the cursor on the screen, it is also necessary to have a web

† NTT Cyber Solutions Laboratories
Yokosuka-shi, 239-0847 Japan

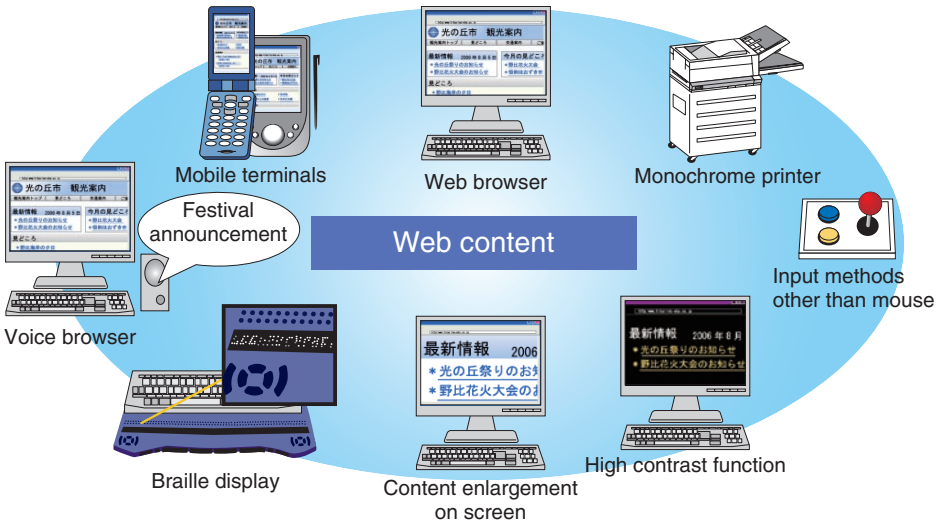


Fig. 1. Web accessibility and various types of ICT equipment.

Table 1. Specific examples of web accessibility problems.

Situation	Problem	Solution
Conversion of information to voice	Because there is no text representation of an image, there is nothing that can be read out, so the image's meaning cannot be understood.	Provide a text description of an image (text alternative).
Conversion of information to voice	When the synthetic voice reads out "red text indicates the current stock prices", no one can understand which of the spoken numbers were red.	Refer to text in a non-visual manner, i.e., without referring to its color.
Conversion of information to voice	Because the information in a table is read out in the order given in the source code, the spoken order is unsuitable and difficult to understand: "time, location, 11 o'clock, Yokosuka".	Arrange information in an order that is understandable when read out such as "time, 11 o' clock, location, Yokosuka".
Display of text	It is difficult to read white text against a light-yellow background.	Use color combinations for text and background that provide enough contrast.
Resizing of text	Enlarging the text size may result in a heading overlapping the body text, making the text difficult to read.	Ensure that text does not overlap when enlarged.
Keyboard operation	If a user uses the tab key to select a part, the focus is trapped within that part.	Enable the focus in a web page to be moved by keyboard operation.

design that can be operated by keyboard alone. A design that supports keyboard operation can also accommodate various other types of input device.

Web accessibility problems related to color occur not only when information is being conveyed by voice, but also when it is printed out on a monochrome printer or when the user has color vision deficiencies. Web designs should consider such problems.

2. Standardization of web accessibility

Guidelines that summarize how best to produce web designs have recently been created and standardized in order to address web accessibility problems. The guidelines that are currently used globally are the Web Content Accessibility Guidelines (WCAG) 2.0 recommended by the World Wide Web Consortium (W3C) [1]. WCAG 2.0 has been incorporated into standards and legislation in many countries and has become a worldwide standard.

WCAG 2.0 has also been adopted in Japan, and JIS X 8341-3 (JIS: Japanese Industrial Standards) was revised accordingly in August 2010 [2]. This standard has two main features: (1) the criteria are explicit, so it is possible to test whether a criterion has been satisfied and (2) there is no dependence on specific coding techniques such as HTML (hypertext markup

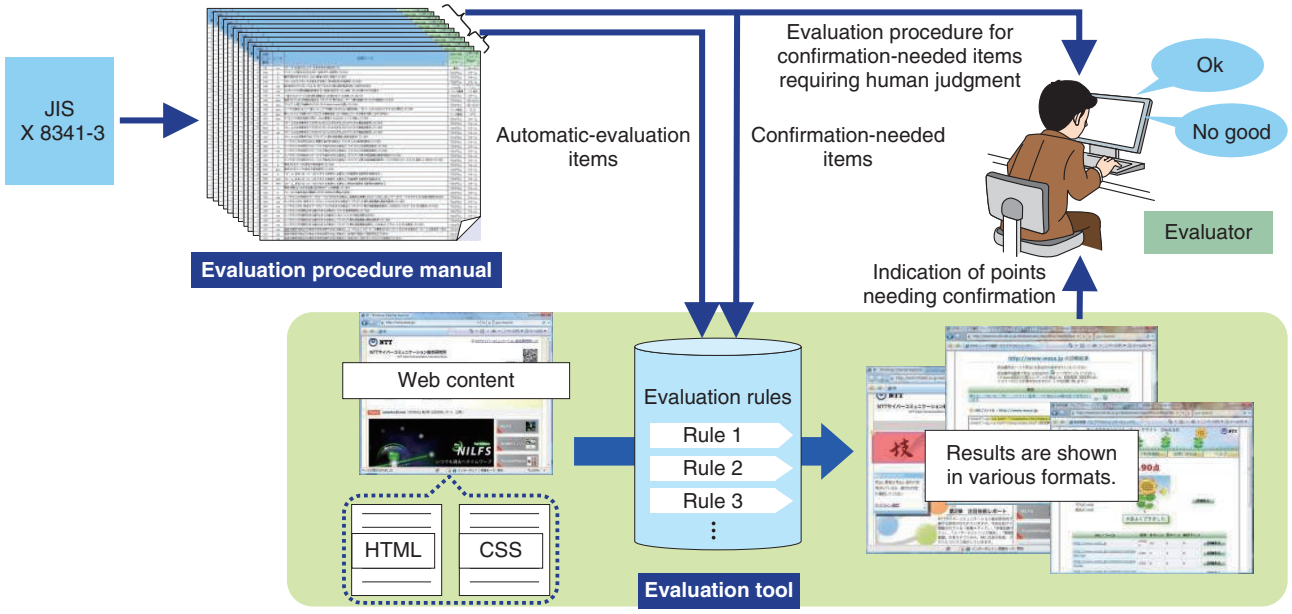


Fig. 2. Relationship between evaluation procedure manual and evaluation tool.

language).

The first feature of JIS X 8341-3 is testability. Among the examples in Table 1 is the problem of low contrast between the text color and background color, which makes the text difficult to read. More specifically, what level of contrast would be sufficient? A formula for calculating contrast is included in JIS X 8341-3, with the criterion being that the result must be at least 4.5:1. Such a criterion is clear, so we can perform an objective test for accessibility.

The second feature is that specific web techniques are not mentioned in the standard. If web techniques were to be mentioned in detail in the standard, the standard would be unable to keep pace with technical advances. The main part of the standard is in terms that can be used even if web techniques progress further, and users can refer to related technical documentation for specific techniques.

W3C has been set up to ensure that web designers can respond to advances in web techniques by creating and updating the related technical documentation. JIS X 8341-3 also refers to the technical documentation related to WCAG 2.0. The technical reference materials to be used along with the JIS standard, such as Japanese translations of WCAG 2.0-related technical documentation, are maintained by the Web Accessibility Infrastructure Committee (WAIC) of the Info-communication Access Council [3].

3. Web accessibility evaluation technology

To create a web design that considers web accessibility, it is necessary to determine whether there is a problem with accessibility and, if so, to adjust the design. Technology for investigating whether or not there is a problem with a web design from the viewpoint of accessibility is called web accessibility evaluation technology. We are deepening our understanding of JIS X 8341-3 by participating in WAIC activities and have been working on the research and development of evaluation technology based on JIS X 8341-3. We have worked on the development of evaluation tools in the past [4], [5], but have changed the evaluation details in line with JIS revisions. We have developed an evaluation procedure manual that summarizes the evaluation procedure using the most recent evaluation tool, which promotes automatic evaluations and confirmations, to enable people who are not particularly familiar with accessibility to perform evaluations simply.

The relationship between the evaluation procedure manual and the evaluation tool is shown in **Fig. 2**. The manual's evaluation items include automatic-evaluation items, which can be evaluated automatically by the evaluation tool according to rules, and confirmation-required items that require human judgment and correction of the tool's rule-based evaluation. For example, if a text description is attached to an image

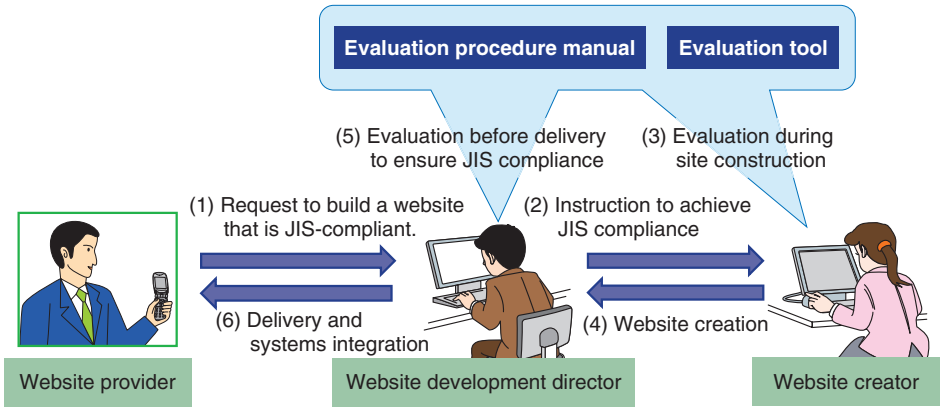


Fig. 3. Example of using web accessibility evaluation technologies.

(text alternative), what the image represents cannot be determined mechanically, although the evaluation tool points out which element need to be evaluated. In such a case, a person (evaluator) must compare and judge the image and the text alternative with reference to the manual. If the text alternative "photograph of the sea" is attached to a photograph of mountains, the text alternative does not reflect the contents of the image, so it is judged not to satisfy the JIS criterion.

The evaluation procedure and judgment criteria are written in detail in the evaluation procedure manual. In addition, a table format is used to enable viewing of evaluation rules at a glance. The evaluation rules can be sorted or filtered, and ease of use during evaluation has been considered.

The evaluation tool is installed on a server and can be used as a web application. Thus, a feature of this system is that it is unnecessary to install the software locally and it is immediately available for use. If the URL (uniform resource locator) of the web page to be evaluated is input into the evaluation tool, the web page's HTML files and CSS (cascading style sheets) files are evaluated according to the evaluation rules.

The tool's evaluation rules were created from the JIS-based evaluation rules in the evaluation procedure manual. The evaluation results are displayed as one of three categories (compliant, noncompliant, or confirmation-required) for each HTML element. Compliant and noncompliant elements are ones where the corresponding JIS criteria are or are not satisfied, respectively. Confirmation-required elements are ones that must be checked by a human evaluator and either confirmed or corrected.

The evaluation tool displays the results in various different formats. A score display giving a summary of the evaluation results, the number of extracted elements corresponding to evaluation rules, and the extraction elements within the HTML source code are highlighted and displayed in red frames within the window displaying the web page. The evaluator can evaluate an image's text alternative by comparing the image displayed on the screen with the text alternative displayed in the source code. A comment page is also provided for each evaluation rule. By referring to the comment pages, a user can gain a deeper understanding of the accessibility.

Our web accessibility evaluation technology is designed for the assumed usage scenario illustrated in **Fig. 3**. A web provider such as an autonomous entity asks a development director in an NTT Group company to construct a JIS-compliant website. The development director tells the web creator to use NTT's web accessibility evaluation manual and tool in order to achieve JIS compliance because it enables even web creators who are unfamiliar with accessibility to create accessibility-friendly pages and learn about accessibility at the same time. This web accessibility evaluation technology is used both during web content creation and during the checking phase after content creation but before delivery to the web provider. We consider that this should be helpful in the production of web content that considers accessibility.

4. Conclusion

The two main reasons that web accessibility is not spreading are a lack of knowledge of methods for considering web accessibility and the cost of web accessibility evaluation. Evaluation by humans takes

time and requires specialist knowledge. In user-centered design, we follow a cycle of observing and interviewing evaluators and then making improvements on the basis of those results and reviewing ways of making the evaluation process more efficient.

At the same time, we must expand our awareness of web accessibility to make it commonplace to consider it instead of refusing to consider it because of the evaluation cost. We participate in the activities of the Japan Web Accessibility Consortium (a nonprofit organization) and are working towards promoting JIS-based web accessibility [6]. We will also continue our research and development of web accessibility evaluation technology in order to create a society in which everyone can enjoy the advantages of networks.

References

[1] Web Content Accessibility Guidelines (WCAG) 2.0. http://www.w3.org/TR/WCAG20/

[2] Japanese Industrial Standards Committee, "JIS X 8341-3:2010; Guidelines for older persons and persons with disabilities—Information and communications equipment, software and services—Part 3: Web content (in Japanese)," Japanese Standards Association, 2010.

[3] Web Accessibility Infrastructure Committee (WAIC) of the Info-communication Access Council (in Japanese). http://www.ciaj.or.jp/access/web/

[4] D. Asai, M. Watanabe, and Y. Asano, "Support Application that Improves Accessibility of Web Contents," Proc. of Working With Computing Systems, 2007.

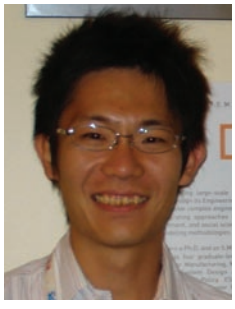
[5] D. Asai, M. Watanabe, and Y. Asano, "Proposal of Method to Improve Web Accessibility by Explaining with Examples (in Japanese)," Human Interface Symposium 2008 Papers, 2008.

[6] Japan Web Accessibility Consortium (in Japanese). http://www.jwac.or.jp/

Masahiro Watanabe

Senior Research Engineer, ICT Design Center, NTT Cyber Solutions Laboratories.

He received the B.E. and M.E. degrees in mechanical engineering and the Dr.E. degree in electronics, information, and communication engineering from Waseda University, Tokyo, in 1991, 1993, and 2003, respectively. He joined NTT Basic Research Laboratories in 1993 and studied the human auditory system. Since moving to NTT Cyber Solutions Laboratories in 1999, he has been studying human-computer interaction, especially universal design and user-centered design. He is a member of the Human Interface Society and the Acoustical Society of Japan.



Daisuke Asai

Research Engineer, ICT Design Center, NTT Cyber Solutions Laboratories.

He received the M.S. degree in mechanical engineering from the University of Tokyo in 2005. He joined NTT Cyber Solutions Laboratories in 2005 as a research engineer and worked on human computer interaction, focusing especially on designing methodologies to enhance web accessibility for disabled and elderly people. From 2010 through May 2011, he was a visiting researcher at MIT AgeLab working on the design of technologies to enhance the quality of life for elderly people living alone.

Harumi Saito

Research Scientist, ICT Design Center, NTT Cyber Solutions Laboratories.

She received the B.A. and M.A. degrees in psychology from the University of Tokyo in 2004 and 2006, respectively. She joined NTT Cyber Solutions Laboratories in 2006, where she worked on graphical user interface design. Her interests include color design and color vision characteristics. She is a member of the Information Processing Society of Japan and the Color Science Association of Japan.

Keiji Morita

ICT Design Center, NTT Cyber Solutions Laboratories.

He received the bachelor's degree in social welfare from Bukkyo University, Kyoto, in 1994. During 1998–2002, he was working in a welfare institution. He joined NTT Cyber Solutions Laboratories in 2005. He is currently engaged in a web accessibility evaluation study.

ICT Service Design for Senior Citizens Based on Aging Characteristics

Yoko Asano†, *Shunichi Yonemura, Akiko Hayashi, and Ryo Hashimoto*

Abstract

In this article, the main problems that senior citizens encounter when utilizing information and communications technology (ICT) services are analyzed from the viewpoints of behavioral and cognitive processing. We introduce the aging characteristics that cause those problems and show how to tackle them in order to implement ICT services that are friendly to senior citizens and will assist and enrich their lifestyles.

1. Introduction

The population of Japan is aging rapidly. The number of adults over the age of 65 (senior citizens) is currently more than 22% of the total population and this figure is expected to exceed 30% by 2025 [1] (**Fig. 1**). In comparison with younger people, senior citizens include more people with failing health. Most senior citizens are losing their motor, perceptual, and cognitive functions because of aging, so they are becoming unable to do things that they could do in the past or they make more mistakes. The effects of these factors are limiting the range of their activities and hindering their everyday lives.

Support through information and communications technology (ICT) services is considered an attractive way of assisting in the lives and activities of senior citizens. The NTT Group is currently planning services such as community revitalization and shopping assistance, using tablet-style terminals that can make use of optical fiber services in a simple manner. However, ICT service utilization has more barriers for senior citizens than for younger people.

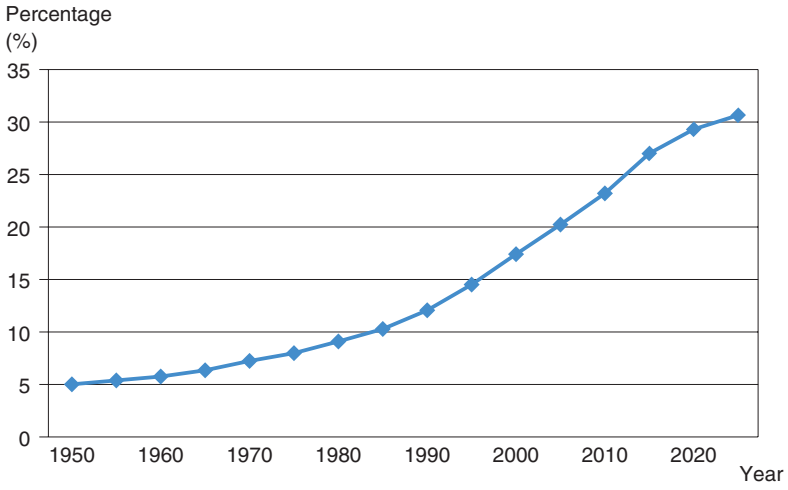
† NTT Cyber Solutions Laboratories
Yokosuka-shi, 239-0847 Japan

2. The importance of design studies for ICT services intended for senior citizens

ICT services have interactive interfaces that require the user to perform some sort of action in most cases. The user must recognize the status of the system and perform some kind of operation in order to make the system perform the desired function. When senior citizens utilize ICT services, they can find them difficult to use, owing to either their aging or their limited experience and knowledge. Such difficulties also depend on the sort of user interface provided by the service. It is therefore important to provide a sophisticated user interface designed taking account of aging and limited experience and knowledge in order to make the service easy to use by senior citizens.

There are a number of guidelines related to user interface design, such as the Introduction to Apple Human Interface Guidelines and the Windows User Experience Interaction Guidelines. However, not much research has been done on designs that treat problems that are specific to senior citizens.

A number of tips have been proposed to create designs intended for senior citizens. However, it is difficult to create a truly effective design if only incomplete information such as “it would be better if the text were larger” is available. It is sometimes



Source: "White Paper on Aged Society, 2010," Japanese Cabinet Office.

Fig. 1. Population trend for those aged 65 and over.

unclear why small text is unsuitable or what sort of problems would be avoided by making it larger. The visual functions of senior citizens deteriorate with age, making it difficult for them to read small characters, but font size is not the only factor influencing readability: another is font contrast. If the original combination of font and background colors is poor, simply increasing the font size will not solve the problem.

Investigations of user interfaces should not attempt to correct interfaces that are problematical by simply tweaking their appearance; it is critical to determine the true causes of the problems, which involve the user's cognitive-behavioral processing abilities. This recommended approach to design requirements will reduce problems in the most effective manner.

3. Problems faced by senior citizens in web utilization

Below, we present some problems that often occur when senior citizens utilize the web. We also introduce the characteristics of senior citizens that cause such problems.

3.1 Problems caused by lack of experience or knowledge

The experience and knowledge necessary for using ICT equipment includes the terminology and general ideas necessary for using services as well as experience with operating similar equipment. Here, we introduce two problems related to terminology and operable objects.

3.1.1 Terminology

We must be cautious about utilizing terminology that is not used much in everyday life, or which is used to refer to a different concept. For example, there have been cases in which "Help" was interpreted as "Rescue me!" and the user did not imagine that it would open a page containing guidance. Moreover, "Home" was interpreted as "one's residence", and the user envisioned that it contained information about the household. In particular, many senior citizens are unfamiliar with many terms written in *katakana* characters. Designers should confirm that *katakana* terms will be well understood before using them.

3.1.2 Operable objects

Most web page contain many links, but many users who are not experienced with web operation do not know which objects can be selected. In addition, there have been many cases in which senior citizens with knowledge of selectable objects failed to apply their knowledge and so failed to access the links that were available. Senior citizens are particularly inexperienced with text links, so they often fail to notice links that are not underlined or ones that differ only slightly in design from ordinary text. In one case, when options were rather far apart, as shown in **Fig. 2**, radio buttons or checkboxes were perceived as just circles or squares and thus overlooked.

An experienced user can recognize selectable

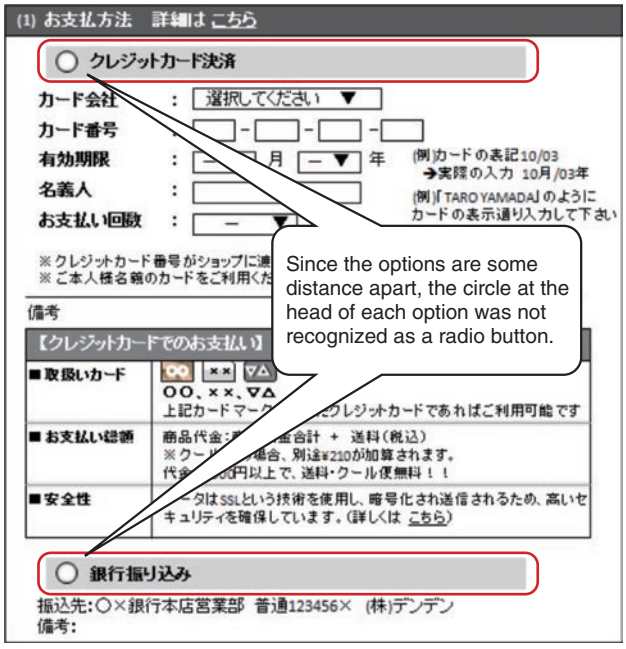


Fig. 2. Example of design in which radio buttons are overlooked.

objects by moving the mouse pointer to hover over different objects in the hope of triggering a change in appearance such as a change in color. Many users who are inexperienced at operating a personal computer (PC), however, have not acquired such identification methods and are uncertain of such input operations. Therefore, it is important to create a design in which selectable locations can be found intuitively, without pointer movement being required.

Moreover, it has been observed that users who have little experience with input operations by keyboard, remote control, or touch panel can experience many problems with key or button inputs. Errors include inaccurate object selection or excessively long pressing. These findings show that the designer must make operations simple and also widen the permissible range of timing and selection areas.

The problems that we have introduced above were taken from current case examples related to senior citizens. Even younger people, who have a lot of experience with PCs and games machines, will become senior citizens in 20–30 years and they can also be expected to suffer aging-related problems with new technologies of that time.

3.2 Problems arising from aging characteristics

Aging refers to the tendency for functions such as perception, cognition, and motility to deteriorate with age. In this section, we introduce *readability* as a problem caused by the deterioration in perceptual functions and also *failure to notice* and *coping with the unexpected* as problems caused by the deterioration in cognitive functions.

3.2.1 Readability

The eyesight of senior citizens deteriorates with age, for various reasons. About 80% of Japanese people in their 60s have cataracts. When eyesight deteriorates, a variety of symptoms occur, such as details becoming difficult to see, colors taking on a yellowish tinge, and the visual field narrowing. For example, a white-and-orange color scheme will be perceived by senior citizens as having an overall yellow tinge and also poor contrast, resulting in it having reduced readability. For that reason, it is necessary to consider readability in detail even in user interface design. Various methods of coping are being considered, such as increasing size and spacing and increasing contrast. It should be noted, however, that increasing the size too much will make the surrounding information difficult to identify.

3.2.2 Failure to notice

Failure to notice desired information even though it has been provided is a problem that is often observed, particularly in senior citizens. It is said that senior citizens have fewer processing resources* [2]. These include the attention function, which directs attention to information needed to achieve an objective without being distracted by unnecessary information, and the working memory, which selects the necessary information and holds it temporarily.

Many case examples involving senior citizens have been gathered. A highly visible area attracts their concentration to the exclusion of other areas [3]. In addition, if a large amount of information is presented all at once, they might be unable to process all of it owing to weak working memory. As countermeasures, there are methods of reducing the amount of information by visually gathering similar pieces of information into a chunk.

If there is a change in only one part of a page containing a lot of information, a senior citizen may be unable to notice the change because a paucity of processing resources. Many case examples have been observed. For example, in the example shown in **Fig. 3**, when a certain category is selected, subcategories appear immediately below it slightly indented.

* Processing resources: The finite amount of mental energy that is shared between information retention and cognitive processing.

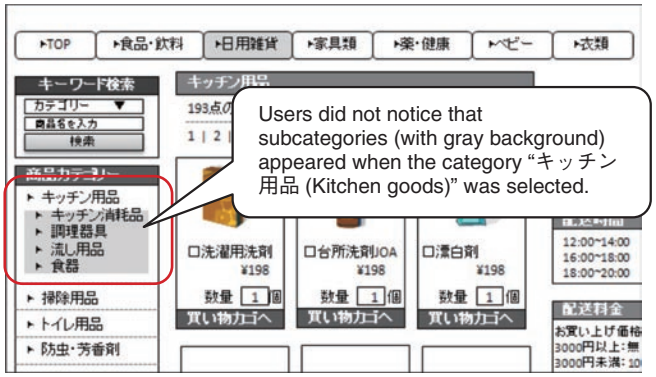


Fig. 3. Example of design in which the existence of lower levels is overlooked.

However, some users did not notice the subcategories [4]. Designers of web pages intended for senior citizens must consider making parts that change more obvious in order to attract attention.

In addition, senior citizens often overlook information that cannot be seen without scrolling, which is thought to be due to insufficient allocation of attention. For senior citizens, information should be accessible without operations such as scrolling as far as possible. And if scrolling is unavoidable, it must be made as intuitive as possible.

3.2.3 Coping with the unexpected

Senior citizens are often observed to be unable to cope with unexpected situations. These problems occur when details that differ from anticipated ones are displayed, unknown terminology is used, or the next operation is not readily apparent. Calmly judging the situation, flexibly changing earlier strategies, and solving problems require advanced cognitive processing abilities such as situational judgment, problem solving, and mental flexibility. However, these abilities are thought to deteriorate with age.

In particular, senior citizens get confused when a motion they made unwittingly is recognized by the system as an input and an unexpected change occurs. We have observed many problems in experiments that examined the use of the iPad. When users touched the touch panel with the palm of the hand or with the hand being used to hold the terminal or when the finger moved while touching the panel, the action was misrecognized as a flick. Such errors are due to weakened control of the fingertips due to deterioration of the motor functions or due to inadvertent contact caused by a poor sense of touch—something that is difficult for a senior citizen to notice. These problems have been observed to be particularly common among senior citizens.

4. ICT service design taking into account aging characteristics

In the previous sections, we examined problems observed in senior citizens when utilizing the web and introduced relevant characteristics of senior citizens. Besides understanding the characteristics of senior citizens, user interface designers should also know what problems that these characteristics will cause.

Solutions can be found for most of the problems caused by perceptional characteristics such as experience, knowledge, or readability, by understanding their relationships with design requirements and considering individual design elements. In some cases, however, a direct solution might lead to a different problem. The design needs to proceed with an integrated viewpoint.

5. Conclusion

Senior citizens have various characteristics and needs, so it is not possible to simply lump them all together by age. Various other factors are thought to be involved, such as health, lifestyle, experience, and knowledge. In the service design, it is difficult to accommodate all senior citizens with a single approach: one must target characteristics and needs under specific conditions. It will be necessary to study whether senior citizens can be classified.

In addition, low service acceptability may result from a reluctance to allow senior citizens a preview of ICT services before they are launched. Acceptability is related to factors such as prejudice against using

ICT equipment or the degree of concordance between the service and the needs. In the future, we will also investigate ICT service acceptability to senior citizens in order to promote the introduction and continued usage of ICT services.

References

[1] The Cabinet Office, "Section 1: The Aging Situation," White Paper on Aged Society, 2010 (in Japanese).

[2] T. Kumada, S. Sudou, and Y. Hibi, "Aging of Attention, Working Memory, and Executive Function, and Cognitive Interface Design for Older Adults," Japanese Psychological Review, Vol. 52, No. 3, pp. 363–378, 2009 (in Japanese).

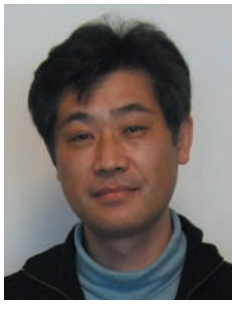
[3] A. F. Kramer, S. Hahn, D. E. Irwin, and J. Theeuwes, "Age Differences in the Control of Looking Behavior: Do you know where your eyes have been?" Psychol. Sci., Vol. 11, No. 3, pp. 210–217, 2000.

[4] A. Hayashi, R. Hashimoto, H. Saito, M. Watanabe, and Y. Asano, "Study on Search Behavior of Older People in Online Supermarket," 2010 HCG Symposium, B6-1, 2010 (in Japanese).

Yoko Asano

Senior Research Engineer, Supervisor, Human Interaction Project, NTT Cyber Solutions Laboratories.

She received the B.E. degree in administration engineering from Keio University, Kanagawa, in 1988 and joined NTT Human Interface Laboratories the same year. She moved to NTT Cyber Solutions Laboratories in 1999. Since then, she has been conducting research on human interfaces. She is a member of the Human Interface Society (HIS), the Japan Ergonomics Society, and the Institute of Electronics, Information and Communication Engineers (IEICE).



Shunichi Yonemura

Senior Research Engineer, Human Interaction Project, NTT Cyber Solutions Laboratories.

He received the B.E. and M.E degrees in engineering from Niigata University in 1983 and 1985, respectively, and the Ph.D. degree in communication science from Waseda University, Tokyo, in 2008. He joined NTT Cyber Solutions Laboratories in 2004. He is currently studying cognitive and social aspects of computer-mediated communication. He is a member of HIS and IEICE.

Akiko Hayashi

Human Interaction Project, NTT Cyber Solutions Laboratories.

She received the B.Sc. degree in engineering science and the M.Sc. degree in biosciences from Osaka University in 2007 and 2009, respectively; she majored in neuroscience and electrophysiology. She joined NTT Cyber Solutions Laboratories in 2009 and is currently studying cognitive psychology and web usability, especially for senior citizens.

Ryo Hashimoto

Human Interaction Project, NTT Cyber Solutions Laboratories.

He received the B.E. degree in engineering and the M.E. degree in communications and computer engineering from Kyoto University in 2008 and 2010, respectively. He joined NTT Cyber Solutions Laboratories in 2010 and is currently studying ICT services usage instructions for elderly people. He is a member of IEICE.

Design Guidelines for Installation Manuals for Novices

Momoko Nakatani†, *Takehiko Ohno, Ai Nakane, and Yoshie Soutome Sagata*

Abstract

This article describes some case studies of designing the paper manual for replacing an Internet router for a home network. Constructing a method for designing easy-to-understand paper manuals for novices is one of the most important tasks at the ICT Design Center. We show how we improved the manual, which is now being distributed to actual users.

1. Introduction

With a greater variety of home appliances being connected to the network, consumers are faced with the daunting task of setting them all up by themselves [1]. Therefore, simplifying this task and providing easy-to-understand manuals to users, especially novice users, are essential tasks for the NTT Group. Since most manuals are currently paper-based ones, this was our focus.

The ICT Design Center has been helping companies in the NTT Group to improve router setup manuals in order to develop guidelines for the creation of user-friendly manuals (ICT: information and communications technology). We have conducted many usability studies in which we gave different setup manuals to novices and observed their actions. Unless we exercise considerable thought and ingenuity in designing the manuals, users are sure to run into some trouble. For example, they are commonly tripped up when the equipment illustrated in the manual does not look exactly the same as the equipment they actually have in front of them. They are also troubled by technical jargon that they cannot understand. Furthermore, users sometimes feel overwhelmed and give up before they even start, or they may plow through the manual and end up skipping over some key information.

† NTT Cyber Solutions Laboratories
Yokosuka-shi, 239-0847 Japan

On the basis of these usability studies, we have made many incremental design improvements and have accumulated essential techniques to reduce the trouble that would otherwise plague users. We have focused on designing a one-sheet manual that places all crucial information on a single piece of paper to simplify the setup. Our challenge was to construct a method for designing easy-to-under paper manuals for novices.

2. Case study

2.1 Device replacement manual

In this article, we consider the specific example of an improved manual for Internet router replacement: replacing an old router with a new one when the old router fails. One might assume that replacing a router would be fairly simple, but in fact all kinds of problems can occur if the manual is poorly designed. For example, how to remove the cover of the connector compartment on the side of the new router and remove the protective shipping cap is illustrated in **Fig. 1(a)**. However, we observed that a surprisingly large number of users could not figure out where the router's cover was. We believe that this was because the figure shows only a closeup view of the location. Our tests showed that users did not experience the same confusion with the improved figure (larger view of the router), shown in **Fig. 1(b)**.

Similarly, we found that just using a closeup view of the socket area to illustrate how to connect the

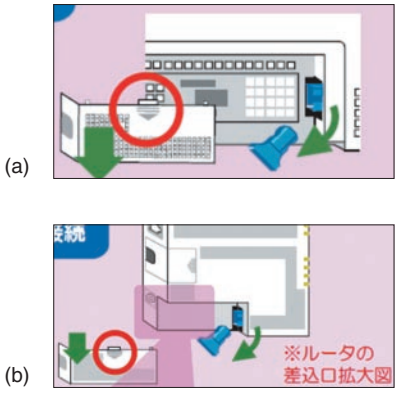


Fig. 1. Figures (caption text omitted here) illustrating how to remove cover and cap: (a) before and (b) after improvement.

router left some users confused. They made mistakes simply because they could not figure out what equipment should be connected to what. In this case, just showing the two pieces of equipment to be connected and the cable together in one figure (telephone, router, and modular cable) eliminated most of the confusion.

These results led us to an important insight and design guideline: namely, that *when inserting figures in the manual, provide an overview that includes the whole configuration*. In this way, we sought to derive general design guidelines from various test cases.

2.2 Two design concepts

Besides the modifications and design fine-tuning already described, we have also conducted studies in which we developed installation manuals according to different design concepts and then compared how users responded to them [2]. The router replacement manuals shown in **Figs. 2** and **3** were developed according to two different design concepts. The text and figures are identical in both manuals: the difference is the layout of this information. Both manuals are also divided vertically into two parts, with the top half showing how to remove the old router and the bottom half showing how to install the new router.

While both layouts were designed on the basis of the abovementioned concept of a whole-configuration overview, the *duplicated-layout* (Fig. 2) was designed so that the subfigures of all connected equipment—e.g., electrical outlet, telephone, and personal computer—are arranged in close proximity around the router. This lets the user see at a glance what equipment the router is connected to. Another feature of this layout is that it reflects the spatial locations of the components. For example, the power connector occupies the top-left corner in both panels (upper panel: old router; lower panel: new router), but the actions for reconnecting the power cord to the new router run from right to left.

On the other hand, in the *ordered-layout manual* (Fig. 3), the procedures for both unplugging cables from the old router and reconnecting them to the new router run from left to right, but the spatial locations of components in the upper and lower panels are reversed. This sequential manual is designed to get the user to perform the steps sequentially from left to right.

2.3 Comparison of the two design concepts

We conducted an experiment in which we asked subjects to replace a router using the two manual types (duplicated-layout manual and ordered-layout manual), and we observed how they went about it. The subjects were divided into two groups of seven people: one group for each manual type. Although both the manuals instructed users to completely disconnect the old router first and then connect the new router, we found that some of the subjects using the duplicated-layout manual went back and forth between steps to disconnect the old router and install the new router with total disregard for the actual sequence of steps. For example, some of the users unplugged the power cord from the old router and plugged it directly into the new router. They next pulled out the local area network (LAN) cable from

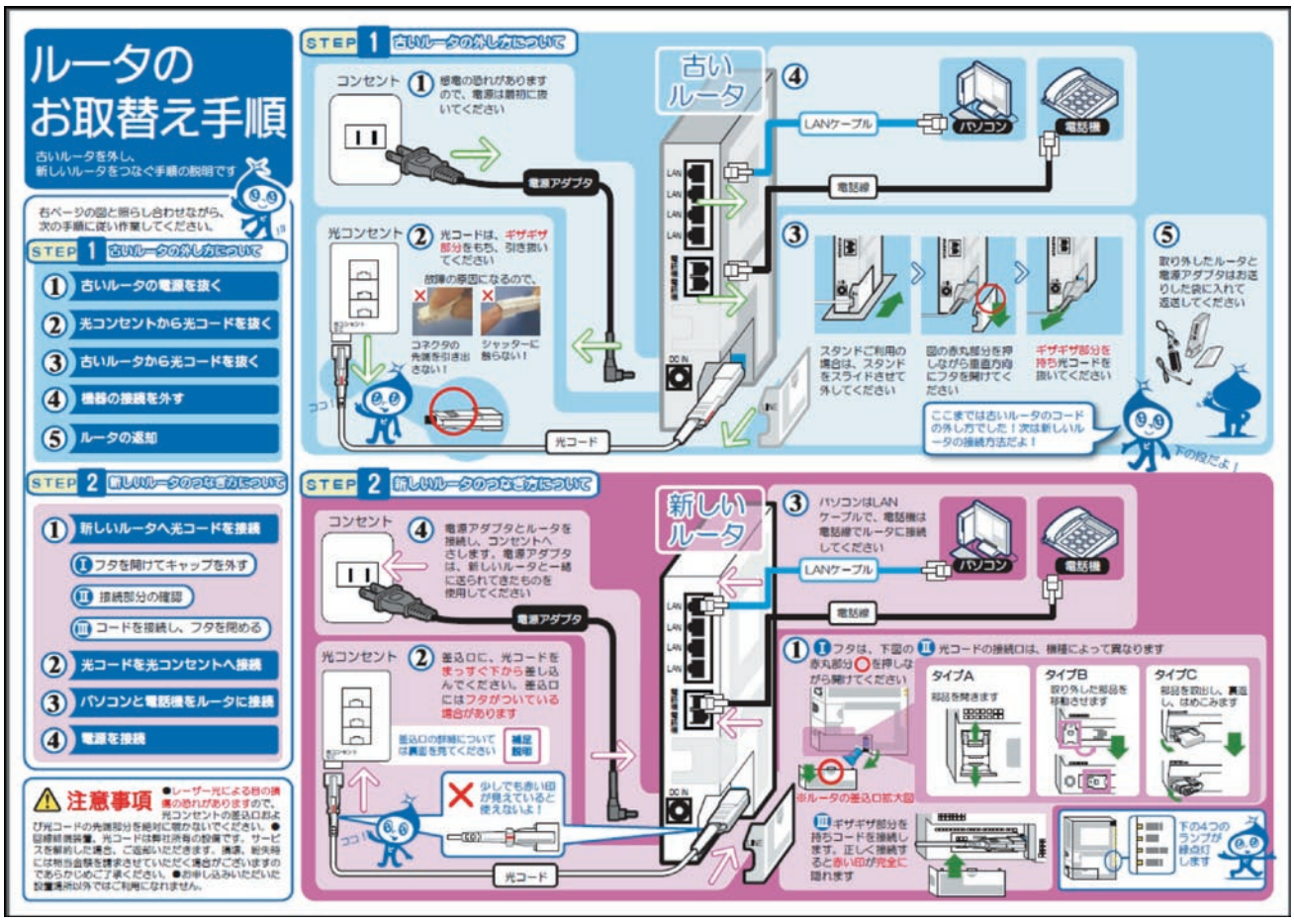


Fig. 2. Duplicated-layout manual.

the old router and plugged it directly into the new router.

We assume that this behavior was motivated by an awareness of the overall objective of the task—that is, unplugging the old router and plugging the cables into the new router—and the users modified the steps in the interest of completing the task more efficiently. In other words, this behavior conforms to the nature of the duplicated-layout manual: easily anticipating the overall task that needs to be done. Note that none of the subjects who used the ordered-layout manual exhibited this behavior of going back and forth between steps to disconnect the old router and install the new router.

Nevertheless, the subjects using the ordered-layout manual did not strictly follow the steps presented in the manual either. They tended to do the tasks involving familiar types of cable first—phone line, LAN cable, and power cord—while putting off the task of dealing with the unfamiliar optical cable* until later. While the cables can be connected in any order without causing any major damage, if they are not connected in the right order the work flow could be disrupted and there might be other consequences.

One thing that we learned from these trials is that if the design goal is to get users to follow steps in exactly the intended order, then not only must the steps be arranged in the correct order, but also additional effort should be taken to ensure that they are followed.

For example, **Fig. 4(a)** shows the figure used to illustrate the task of *removing the cover and plugging*

* Optical cable. The optical cable plug is very different from a conventional telephone cable plug in terms of shape and handling. Many of the manual's target users will never have seen an optical cable before even though they are replacing a router because, in many cases, the original router was installed by a service engineer.

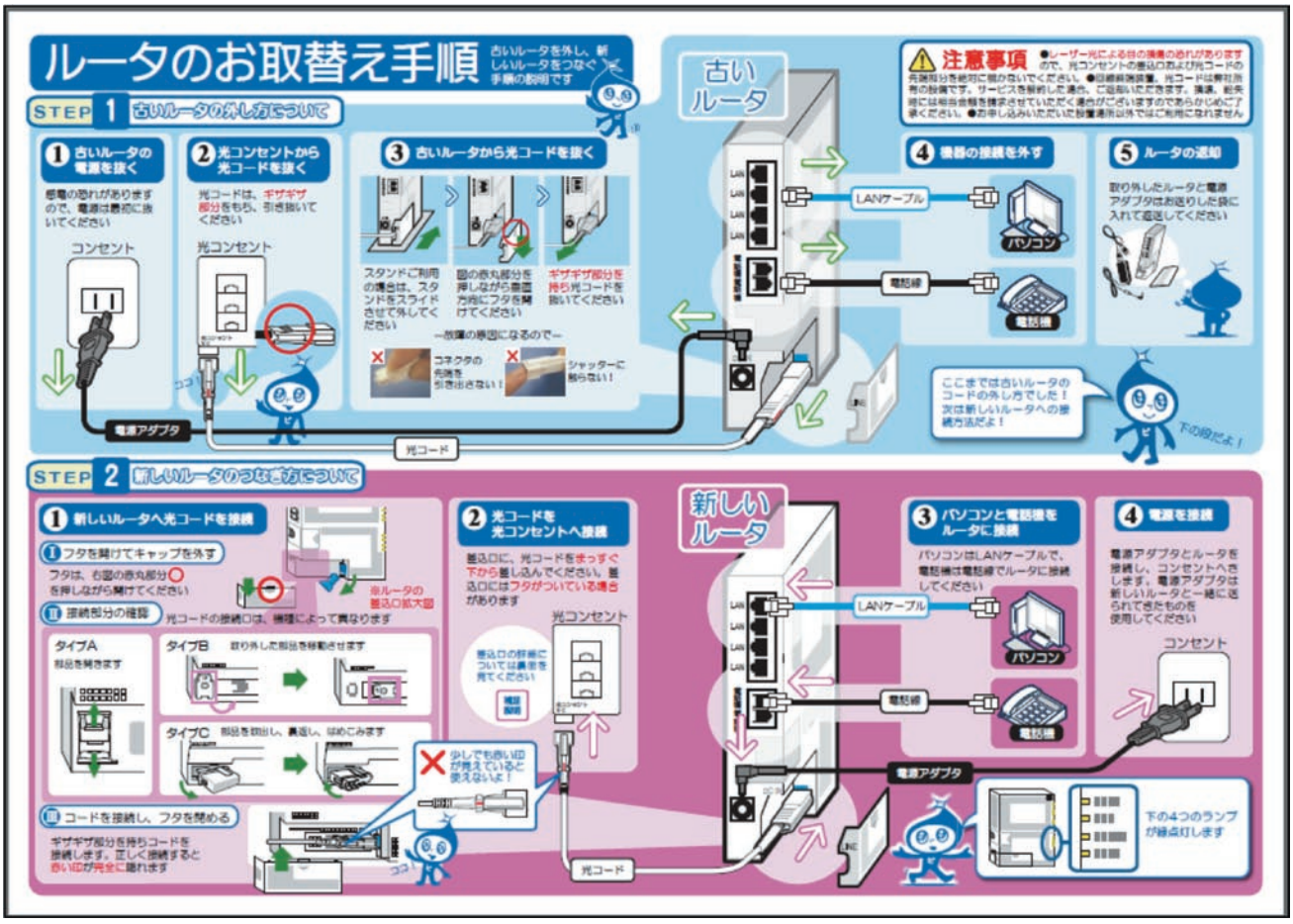


Fig. 3. Ordered-layout manual.

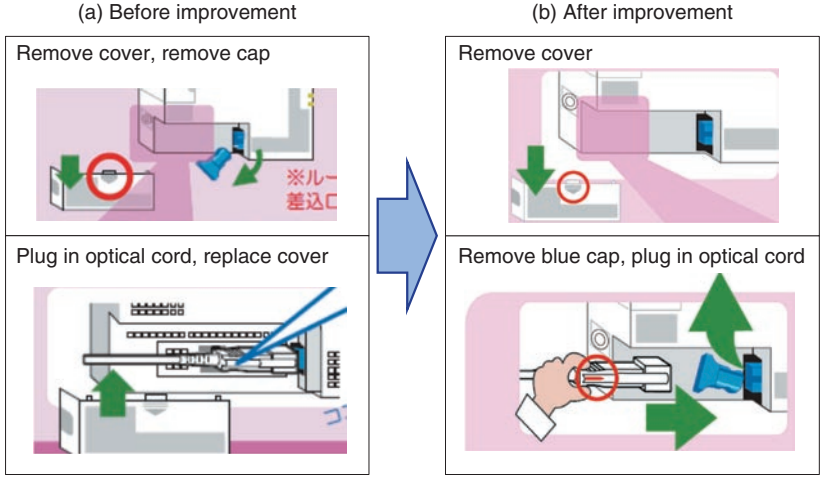


Fig. 4. Figure illustrating the actions: remove cover, remove cap, and plug in optical cord.

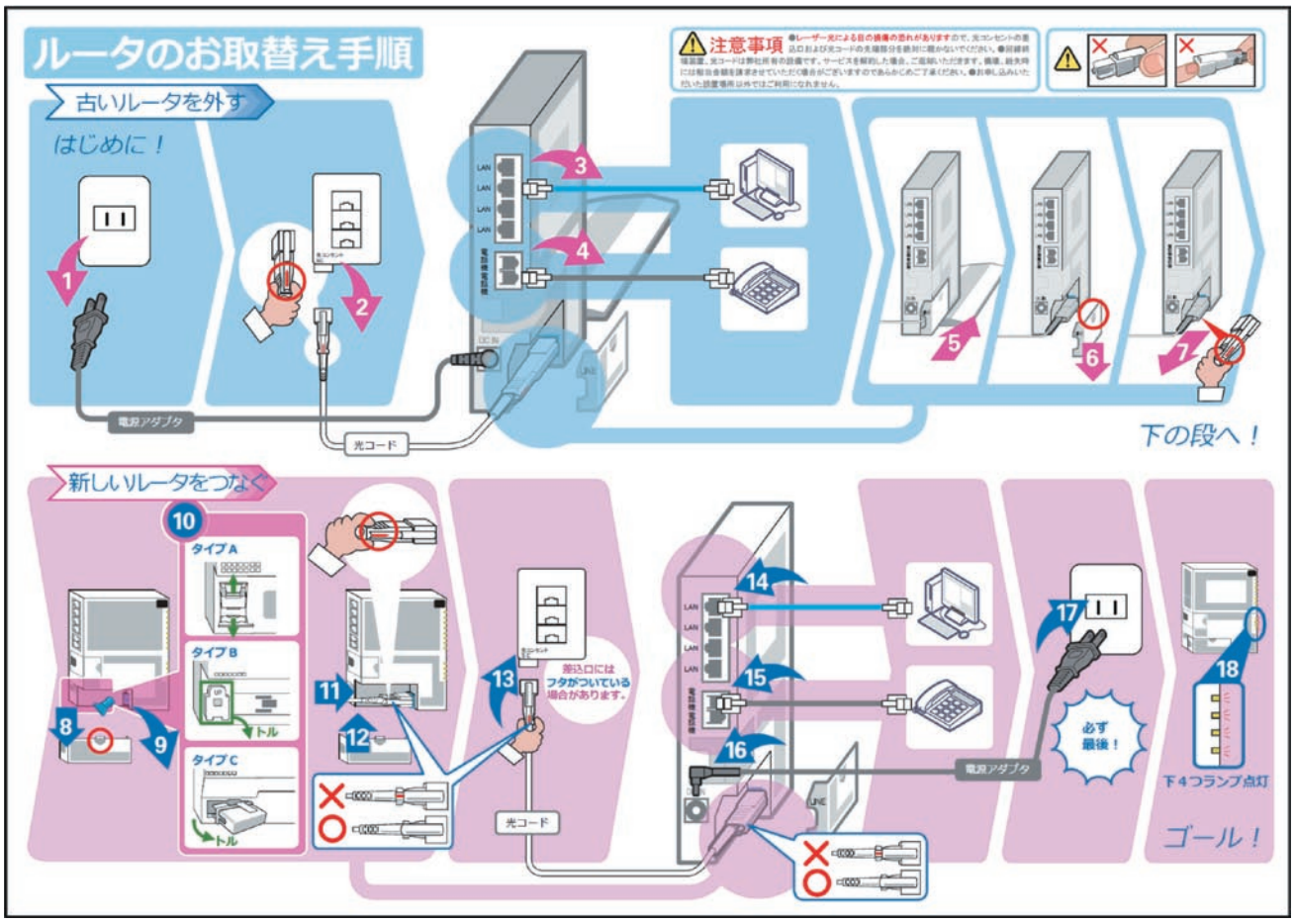


Fig. 5. Installation guide with much less text.

in the optical cord in the trials. The cap should be removed before the optical cord is plugged in, but we observed quite a few users who did not follow these instructions. We observed that many tried to plug the optical cord in by pushing it into the cable compartment without removing the cap; this could damage the optical cable and will fail to achieve a good connection, but in the experiment, no one actually damaged the cable. We then came up with an improved illustration shown in **Fig. 4(b)** that gets users to follow the procedure by illustrating the procedures for removing the cover and plugging in the optical cord in a single figure. The main difference between (a) and (b) is that in (a) *remove cover* and *remove cap* are illustrated in one picture and *plug in optical cord* is illustrated in the second picture. On the other hand, in (b) *remove cover* is illustrated in one picture and *remove cap* and *plug in optical cord* are illustrated in the second picture. Our aim with the improved design (b) was to get users to realize that you cannot insert the optical cable until after the cap has been removed.

In addition, we further improved the ordered-layout manual, as shown in **Fig. 5**, by minimizing the amount of text and emphasizing the sequence numbers of the steps. Here, we took the *minimalist approach* [3] that is commonly used in software manuals. If you try to explain every conceivable function and operation in a software manual, you can end up with a manual as thick as a telephone book, so the minimalist approach offers a way to cut out a lot of inconsequential excess information. While the minimal software manual enables users to actively learn a wide range of functions and procedures, the simplified replacement manual (minimalistic manual) should help reduce the feeling of aversion toward this kind of task.

The effects of these proposed improvements are

now being studied, but one thing is certain: good design requires considerable ingenuity so that users are guided to execute the actions intended by designers.

3. Conclusion

In order to design user-friendly easy-to-understand installation manuals, it is important to thoroughly understand the users. Yet no matter how well one tries to understand the people who will be using the manual, some of them will act in ways not anticipated by the designers or authors of the instructions, so coming up with the ultimate perfect design solution in one try is practically impossible. In order to develop well-designed installation manuals, we continue to make repeated incremental improvements while periodically assessing user responses.

It is also necessary to sift through the content and determine what is truly important in terms of the task at hand. In the examples presented here, the duplicated-layout manual proved advantageous in that it enabled users to easily anticipate the overall task that needed to be done, but the ordered-layout manual proved better at getting users to follow the steps in the intended order. The designer should understand the advantages of each type and choose the layout according to the situation.

At the ICT Design Center, we are striving to improve the quality of product manuals, equipment installation manuals, and other instructional materials through user observation and assessment. Building on what we have achieved so far, we will continue to collect data and best design practices necessary to create user-friendly easy-to-understand installation guides.

References

[1] T. Ohno, M. Nakatani, A. Nakane, and Y. Cen, "When People Feel Distraction: Measurement and Understanding of Distraction During Setup Task of Information Appliances," IEICE Trans. on information and systems, Vol. J94-D, No. 1, pp. 94–106, 2011 (in Japanese).

[2] M. Nakatani, A. Nakane, Y. Katagiri, T. Ohno, and S. Hashimoto, "One-sheet Manual Design that does not Mislead Users," Proc. of the 139th Forum of the Human-Computer Interaction (HCI) SIG, the Information Processing Society of Japan, July 19, 2010 (in Japanese).

[3] J. M. Carrol, "The Nurnberg Funnel: Designing Minimalist Instruction for Practical Computer Skill," The MIT Press, June 1990.

Momoko Nakatani

Research Engineer, Human Interaction Project, NTT Cyber Solutions Laboratories.

She received the B.Sc. and M.Sc. degrees from Waseda University, Tokyo, in 2001 and 2003, respectively. She has been researching human-computer interaction, human-centered design, manual design, human modeling, usability, and qualitative studies. Her research focuses on establishing a method to support novice ICT users. She is a member of the Association for Computing Machinery (ACM), the Information Processing Society of Japan (IPSJ), and the Human Interface Society.

Takehiko Ohno

Senior Research Engineer, Supervisor, Human Interaction Project, NTT Cyber Solutions Laboratories.

He received the B.Sc. and M.Sc. degrees from Tokyo Institute of Technology in 1992 and 1994, respectively. He joined NTT Basic Research Laboratories in 1994 and studied cognitive science and human-computer interaction. He has been researching human-computer interaction, human-centered system design, user experience design, usability, gaze tracking technology and its applications, cognitive modeling, information appliances, and computer-mediated communication. He is a member of ACM, IPSJ, the Japan Cognitive Science Society, and the Institute of Electronics, Information and Communication Engineers.

Ai Nakane

Researcher, Human Interaction Project, NTT Cyber Solutions Laboratories.

She received the B.Sc. and M.Sc. degrees from the School of Education, Graduate School of Education and Human Development, Nagoya University in 2006 and 2008, respectively. She has been researching human-centered design, user-interfaces, and user experience. She is a member of the Japanese Psychological Association.

Yoshie Soutome Sagata

Researcher, Human Interaction Project, NTT Cyber Solutions Laboratories.

She received the B.Sc. and M.Sc. degrees from the University of Tsukuba, Ibaraki, in 1992 and 1994, respectively. She has been researching human-centered system design and usability.

Efforts to Minimize Human Errors in Network Maintenance

Takehiko Ohno†, Momoko Nakatani, Chihiro Takayama, and Kouki Kusano

Abstract

We describe recent efforts to reduce human error in network maintenance work. Through careful observation and analysis of maintenance work conducted according to a procedure manual, we have been able to identify a number of hidden risk factors in the way that work is carried out.

1. Introduction

Providing robust, reliable network facilities is one of NTT Group's most important priorities and NTT's various divisions and departments strive to provide customers with services that are safe and secure. Network maintenance is particularly important and involves various operations: repairing network facilities that have failed, deploying new ones, and decommissioning ones that are no longer required. Human error in performing these various tasks can adversely affect networks—even causing them to crash in the worst case—so efforts to mitigate and prevent errors are extremely important. Here, we introduce the role of NTT's ICT Design Center (IDeC) in reducing human error, taking as an example the network maintenance task of decommissioning leased-line networks (ICT: information and communications technology). Operating companies have already done a fairly good job of reducing human errors by developing procedure manuals for conducting maintenance work, by adopting procedures that incorporate double and triple checks, and by applying many other measures. IDeC wants to cut human errors to the bare minimum and is now working with operating companies to prevent errors by identifying hidden risk factors that still exist in current measures and procedures.

† NTT Cyber Solutions Laboratories
Yokosuka-shi, 239-0847 Japan

2. Why do human errors occur?

Let us briefly consider why human errors occur in the first place. It is often said that people make mistakes, and that mistakes can never be entirely eliminated. So does this mean that errors are inevitable? Far from being unforeseen one-time events, most human errors have been found through studies to be similar to errors that have occurred in the past. Nor are they minor inconsequential mistakes: more often than not, human errors are serious blunders made repeatedly by experienced, well-organized people [1]. In other words, most human errors have occurred in the past and are likely to reoccur in the future. Another fallacy is that errors are avoided by those familiar with the job. Let us begin by sorting out two types of factors that are involved: factors that make human errors more likely to occur and external factors related to multiple people working together.

The types of human errors that are likely to occur and the factors that contribute them are shown in **Fig. 1**. The more likely types of error to occur certainly vary with the job, but people are the source of various types of errors. In particular, slip-ups where an omission or action leads to the wrong conclusion even though the person thinks the procedure has been executed correctly [2] are commonplace (we have all had the experience of calling someone by the wrong name without realizing it). And when one is faced with a difficult situation that one rarely encounters, mistakes are sometimes made as a result of a faulty hypothesis or wrong understanding of the system

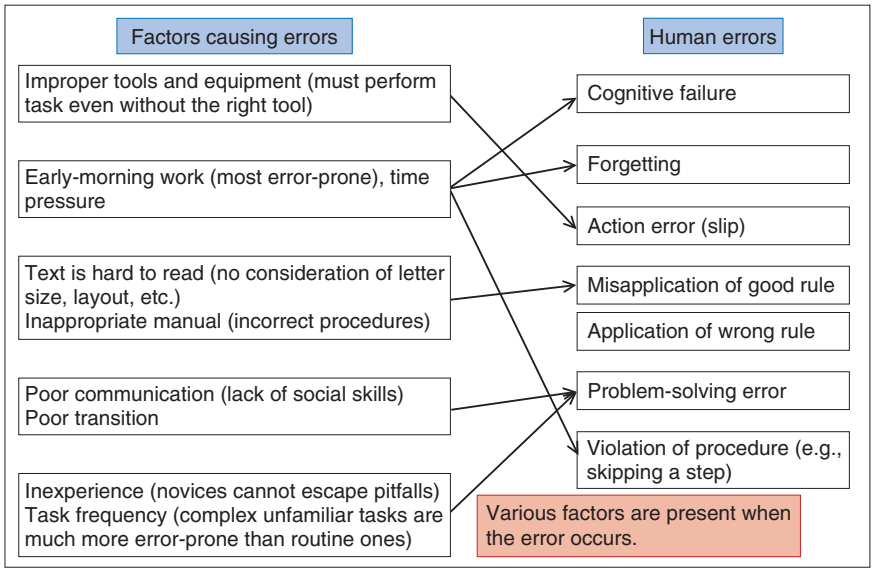


Fig. 1. Human errors and factors likely to cause them (modified from ref. [1]).

structure. This is called a problem-solving error. Errors of this type are more prevalent among novices and becomes less frequent as a person gains experience and skill.

Errors originate in peoples' minds, but their incidence and likelihood are increased by various external factors. For example, improper procedures or manuals can lead to errors. Working at the crack of dawn or under other non-ideal conditions, such as when dealing with multiple problems or when pressed for time, can also contribute to errors. Preventing errors from occurring in the human mind in the first place is obviously very difficult, but figuring out what types of factors occur during a particular task is the first step in reducing human errors.

3. Identifying human error risk factors by onsite observation

Here, we consider human errors associated with the task of decommissioning leased-line networks, or more specifically, removing optical network units (ONUs) and other network equipment connected to leased lines that are no longer being used. An error could have a huge impact since removing the wrong device or cable could interrupt other leased-line services, so efforts to prevent errors are extremely important.

Strict procedures have been established for doing this work, and technicians are required to follow them to the letter. If a problem occurs, the technician must stop work immediately and consult a controller back at the maintenance center, who delivers sequential instructions from the procedure manual over the telephone. The controller also monitors leased-line alarms, a system that alerts personnel the instant that a problem occurs (**Fig. 2**).

With the idea of cutting back on human errors even more, we visited actual leased-line removal sites to observe technicians at work with the procedure manuals to see if we could discover any concealed risk factors using the steps outlined in **Fig. 3**. First, the leader in charge of orchestrating the work gave us a detailed demonstration of what the work entails at the training facility, while also providing a detailed explanation of why the work needs to be done.

Next, we closely analyzed each work phase using the procedure manual: perception (visual inspection), cognition (mental rehearsal), and action (manual or verbal actions). On the basis of the results of this preliminary assessment, we then considered how the technician's attention varied throughout the procedure, whether the work could be done according to procedure while letting go of the cable, and so on.

Having gained a good understanding of the significance and purpose of the work through the above steps, we then interviewed the technicians and observed them work at actual worksites (typically datacenters). In the interviews, the technicians generally just reiterated the standard procedure, but we

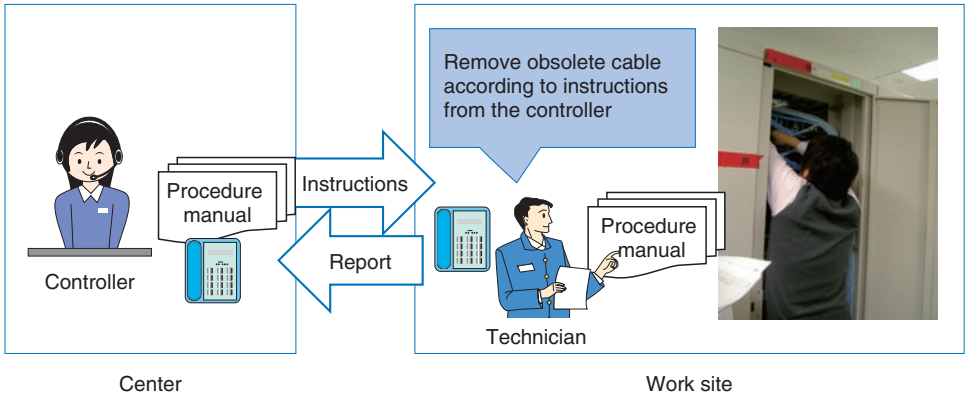


Fig. 2. Decommissioning a leased-line network.

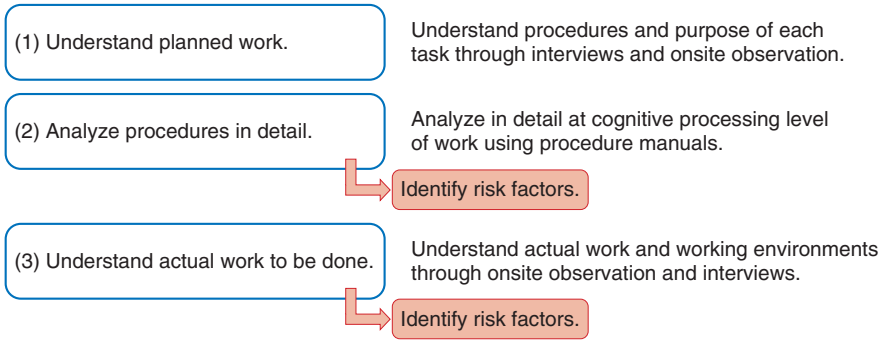


Fig. 3. Identification of human error risk factors.

asked them picture in their minds how they had actually done the work in the past and to reproduce that actual procedure in as much detail as possible.

Operating companies have already implemented many measures that have sharply reduced the incidence of human error. When we began this project, we expected to face a daunting task and that further reducing the incidence of human errors might be like trying to squeeze water from a stone. It all depended on going back to the starting point of human-centered design and observing from the perspective of the technicians themselves how the work was actually done.

4. Extracted risk factors

There are two aspects of leased-line decommissioning work where human errors can be reduced: (1) in the preparation of the procedure manual that is used simultaneously by the controller and the technician and (2) during the two-way communication over the telephone between the controller and the technician. As one can see in **Fig. 4**, our study revealed that there are potential risk factors in both of these aspects.

The purpose of having the controller and technician use the same procedure manual is to prevent mistakes and make sure that no procedural steps are skipped. From the interviews, we found that the procedures for this decommissioning task were fairly constant, and since the technicians receive instructions one step at a time from the controller over the telephone*, they do not feel that it is necessary to follow their own copy of the manual closely as they work. We also identified certain risks associated with using the procedure

* The telephone used for this communication is usually a landline. Mobile phones cannot be used because of the high noise levels at the work site. Moreover, there are few circumstances where technicians can use hands-free headsets, so they may have to wedge the telephone handset between ear and shoulder while using both hands for the work.

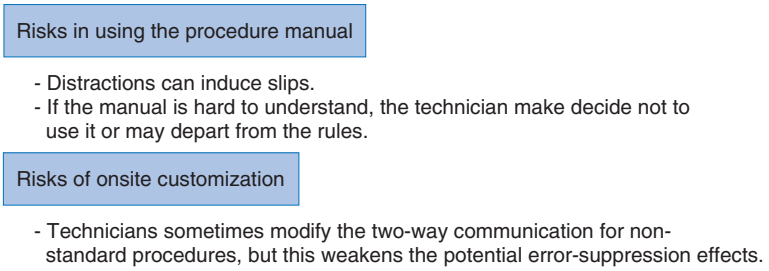


Fig. 4. Identified risk factors.

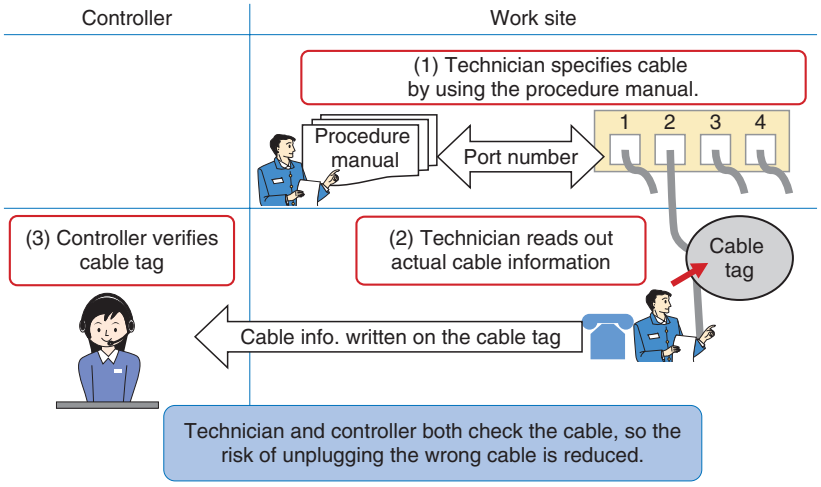


Fig. 5. Significance of two-way communication.

manual. For example, technicians must keep their eyes and hands on the cable at all times as they pull it out, but if they are trying to follow along in the manual at the same time, there is a good chance that their eyes will stray or that they will let go of the cable as they turn the page. People cannot consciously focus on more than one thing at a time, so the manual tends to draw attention away from the cable. For technicians, the advantages of using the manual must outweigh the disadvantages of using it. We must come up with a way of using the manual that minimizes the risks while maximizing the advantages.

The significance of the two-way communication routine is illustrated in **Fig. 5**. First, the technician grasps the cable to be removed and reads the attached cable tag (a small tag that lists the cable number and other information) to the controller, who verifies that the number is correct. In this way, the controller should catch the error even if the technician inadvertently selects the wrong cable. After confirming that the right cable has been selected, the technician marks it with colored tape and eventually pulls it out (sometimes immediately but other times after doing another job somewhere else). The most important point is that the cable to be removed is positively identified. Would making the job into two-person operation cut down on human errors? One technician could actually pull out the cable and the other could converse with the controller on the phone. However, in the unlikely but entirely possible case that the cable-handling technician inadvertently took hold of the wrong cable, this error could easily go undetected. The whole point of the two-way communication, which aims to reduce errors at the worksite, would be lost by making it into a two-person operation; hence, it would increase the risk factor.

A clear understanding of the work environment is also important for assessing human error risk factors.

For this particular task, the work is much more difficult if cables are densely packed in a confined space; touching another cable involves a risk of adversely affecting its performance. Depending on the cable's position, the technician may have to get down on hands and knees or climb a ladder to do the work, while keeping hands and eyes on the cable. Moreover, it is often hard for technicians to hear and be heard over the noise of air conditioners at datacenters, so information might be conveyed incorrectly over the phone (when people hear speech mixed with noise, they naturally tend to make up words that they think fit the context even when they cannot really hear them, and this is also a risk factor). It is apparent that even when work seems relatively simple for technicians, its cognitive process is complicated and imposes a high mental workload. To prevent errors in environments such as these, personnel must know which parts of the procedures are really important and why.

5. Error mitigation recommendations

On the basis of the above analysis, we proposed a number of design changes to the procedure manual while reinforcing the principle objective of two-way communication. First, regarding the procedure manual, rehearsing procedures in your mind as you approach a task is a useful way to reduce errors, so we proposed changes that enable the technician to get an overview of the task by stealing quick glances at the manual while focusing on the task at hand. Specifically, we proposed

- adding schematic figures at the top of each page showing the entire configuration in addition to the current step addressed on the page,
- adding warnings at key points: "Keep your hands on the workpiece at all times!"
- increasing the font size and adding variety on the page,
- adding break points that let technicians catch their breath before tackling riskier procedures, and
- changing the layout so that technicians can fold the manual in half.

We also made the manual easier for controllers to understand and highlighted points that they should be aware of. The operating companies have adopted our recommendations and plan to switch over to technician-friendly manuals in the near future.

We noted that the primary purpose of the two-way communication is to enable the technician doing the actual work to verify that he or she has the right cable without taking his or her hands and eyes off the cable. A reduction in human error is obviously not something that can be achieved immediately, but something that requires repeated effort from various standpoints. The proposals described here can also be incorporated in various well-known approaches to help reduce human errors over the long term.

6. Conclusion

In this article, we introduced the role of the ICT Design Center (IDeC) in mitigating human error, taking as an example the maintenance task of decommissioning leased-line networks. A number of other divisions are engaged in similar work. While the specific tasks and environments differ, they all involve people performing work. IDeC remains committed to initiatives based on a deeper understanding of the environments that surround people.

References

[1] J. T. Reason and A. Hobbs, "Managing Maintenance Error: A Practical Guide," Juse Press, Ltd., 2005.
[2] D. A. Norman, "Categorization of Action Slips," Psychological Review, Vol. 88, pp. 1–15, 1981.

Takehiko Ohno

Senior Research Engineer, Supervisor, Human Interaction Project, NTT Cyber Solutions Laboratories.

He received the B.Sc. and M.Sc. degrees from Tokyo Institute of Technology, in 1992 and 1994, respectively. He joined NTT Basic Research Laboratories in 1994 and studied cognitive science and human-computer interaction. He has been researching human-computer interaction, human-centered system design, user experience design, usability, gaze tracking technology and its applications, cognitive modeling, information appliances, and computer-mediated communication. He is a member of the Association for Computing Machinery (ACM), the Information Processing Society of Japan (IPSJ), the Japan Cognitive Science Society, and the Institute of Electronics, Information and Communication Engineers.

Momoko Nakatani

Research Engineer, Human Interaction Project, NTT Cyber Solutions Laboratories.

She received the B.Sc. and M.Sc. degrees from Waseda University, Tokyo, in 2001 and 2003, respectively. She has been researching human-computer interaction, human-centered design, manual design, human modeling, usability, and qualitative studies. Her research focuses on establishing a method to support novice ICT users. She is a member of ACM, IPSJ, and the Human Interface Society.

Chihiro Takayama

Researcher, Human Interaction Project, NTT Cyber Solutions Laboratories.

He received the B.Sc. and M.Sc. degrees in computer science from Waseda University, Tokyo, in 2007 and 2009, respectively. He has been researching human-computer interaction, human-centered design, usability, and cognitive engineering. He is also interested in information appliances, pervasive computing, and persuasive technology.

Kouki Kusano

Researcher, Human Interaction Project, NTT Cyber Solutions Laboratories.

He received the B.Sc. and M.Sc. degrees in computer science from the University of Electro-Communications, Tokyo, in 2008 and 2010, respectively. He has been researching human-computer interaction, human-centered design, usability, and cognitive engineering. He is also interested in user interface design methodology.

Quantum Key Distribution Technology

Yasuhiro Tokura†

Abstract

Quantum key distribution provides the highest security in the communication channel by using the principle of quantum mechanics. This article briefly reviews recent trends of this technology and the status of NTT's research. The following articles give more details.

1. Introduction

Quantum mechanics, born in the early 20th century, has established itself as the fundamental principle controlling various types of nanoscale physics, from electronics as in transistors to molecules and biomaterials. In the 20th century, another rapidly developing field emerged: information and communications technology (ICT). Recently, much attention had been attracted to a new research field, quantum information and communications technology (QICT), which is based on these two seemingly barely interrelated fields. QICT provides a deeper understanding of quantum mechanics via new approaches for verifying its principles, as well as completely new functionalities that cannot be realized by *classical* ICT, for example, enabling us to solve extremely difficult problems in a short time by using quantum computers and to have completely secure communication by quantum key distribution and quantum certification. Among different quantum media from elementary particles to macroscopic quantum states such as superconducting states, the quantum of light, the photon, is the most suitable candidate for quantum communication. The most fundamental form of quantum communication, quantum key distribution (QKD), enables secret keys to be shared between two remote parties through the sending of photons with information encoded on them. The significant feature of this technology is that the act of eavesdropping can be detected, which is almost impossible in conventional communications.

† NTT Basic Research Laboratories
Atsugi-shi, 243-0198 Japan

2. Short history of QKD

The risk of the digital data exchanged over the modern Internet being stolen or eavesdropped upon cannot be diminished to zero. Therefore, the technology of cryptography is used when people send passwords or credit card numbers. Widely used is the public key cryptosystem: its security is based on certain hard mathematical problems. Therefore, the strength of its security depends on the development of computer performance and mathematical algorithms. In contrast, the one-time pad cryptosystem has long been known to be impossible to break. However, two parties (a sender called Alice and a receiver called Bob) need to share secret keys that are completely random, the same size as the message to be sent, and never used again. QKD can provide a method of distributing such keys in an ultimately secure manner. The basic principle of QKD is depicted in **Fig. 1**. Alice prepares a long random bit array made of 0s and 1s and encodes this binary information on photons, which are sent to Bob through a quantum channel (e.g., an optical fiber). Bob obtains a logical bit array by measuring each photon. So far, this seems the same as classical communications, but a difference becomes evident when an eavesdropper tries to steal the bit information. In classical communication, the classical information can be stolen by branching part of it. But the quantum information encoded on an elementary particle, a photon, cannot be divided any more: the only choices are to take it all or leave it all. The stolen data is equivalent to simple loss, and the remaining random bits can be used as a secret key if Bob later tells Alice the positions of the bits that he knows have been lost. A clever eavesdropper might send fake photons that depend on the measured

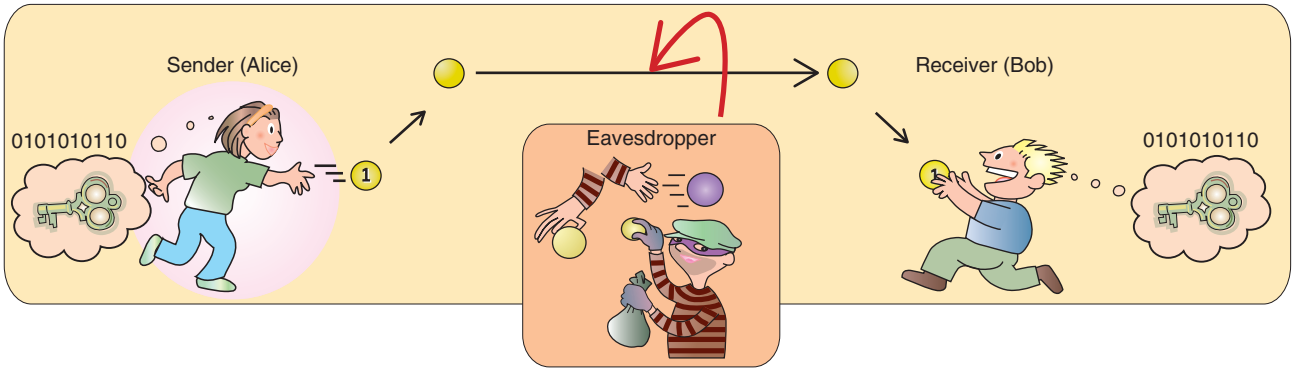


Fig. 1. Principle of quantum key distribution.

results of the stolen photons. However, one cannot measure a photon quantum state without changing it in an uncontrollable manner (measurement back-action), so the fake signals depending on this measurement inevitably introduce bit errors into Bob's measurements. The no-cloning theorem of quantum mechanics prohibits the eavesdropper from making a copy of a photon before measurement. Therefore, the eavesdropper cannot obtain the key information without inducing bit errors. In other words, Alice and Bob can recognize the presence of an eavesdropper by checking the bit errors.

In the first QKD protocol proposed in 1984, called BB84 after the proposers C. H. Bennett and G. Brassard, Alice assigns logical bits 0 and 1 to a polarization state of a photon using two randomly chosen sets (bases), namely, circular polarizations (right-hand circular and left-hand circular) or linear polarizations (horizontal and vertical). Bob measures the photon after choosing the measurement basis at random, but he obtains the correct result only if he has chosen the same basis as Alice. Therefore, after photon transmission, Alice and Bob exchange information about their bases and sift out only the key for that corresponds to the same basis. They compare part of the obtained sifted key to check the error rate. If the error rate is less than a certain threshold value, they can conclude that no eavesdropper is present. Finally, a secure key is generated with post-processes—error correction and privacy amplification—to diminish information that might leak to an eavesdropper.

Unconditional security proof, which certifies secure key distribution even when an eavesdropper tries all physically allowed actions, has been known for the BB84 protocol when we can use an ideal single-photon emitter that emits photons exactly one-by-one. More recently, unconditional security has been proven for an attenuated coherent (laser) source, instead of a single-photon emitter, with the use of an additional procedure (decoy-BB84). Other QKD protocols than BB84 have also been proposed and their security has been investigated.

Optical fibers have been the most popular quantum channel to date, but the polarization states, which were initially proposed in BB84, cannot be maintained stably over a long distance. Instead, as shown in **Fig. 2**, the time-bin basis (a photon is in either the first or second pulse) or the phase basis (the relative phase of a photon extending over two pulses is either 0 or π) can be used. Alternatively, one can use two bases of relative phases $\{0, \pi\}$ or $\{\pi/2, 3\pi/2\}$.

In real systems, the secure key's generation rate and distribution distance are limited by the sensitivity, dark count rate (rate of signal detection without actual arrival of photons) of the single-photon detector (SPD), and the loss of the quantum channel. How far can we distribute a secure key? When we use optical fibers, we need to use photons with a wavelength of 1.5 μm since that has the minimum transmission loss. The biggest technical issue has been the lack of an adequate SPD sensitive to photons of this wavelength. However, the recent development of SPDs has enabled 1-Mbit/s secure key generation for 50-km transmission through fiber [1] or 200 km if the key generation rate is very slow [2], [3]. Although much longer transmission with further-improved SPDs may be difficult, there are three possible solutions. One is to locate trusted relay points every 50–100 km and share the secret key between two distant points by exchanging keys at the relay points. Field testbed experiments were demonstrated in 2008 by the EU's SECOQC project [4] and also in 2010 by the Tokyo

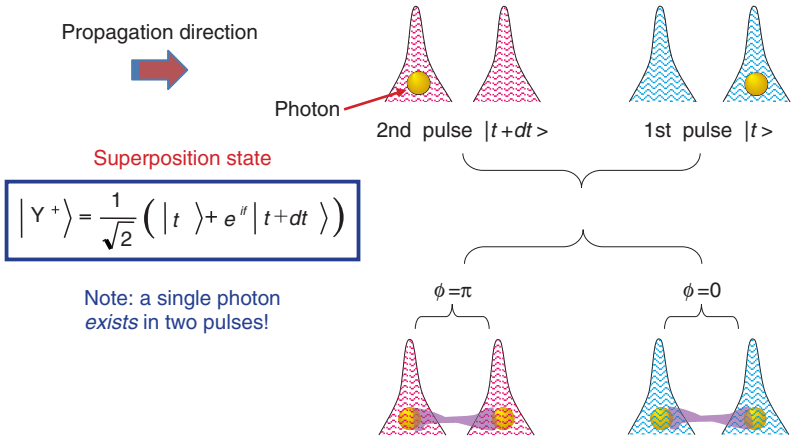


Fig. 2. Time-bin basis and phase basis.

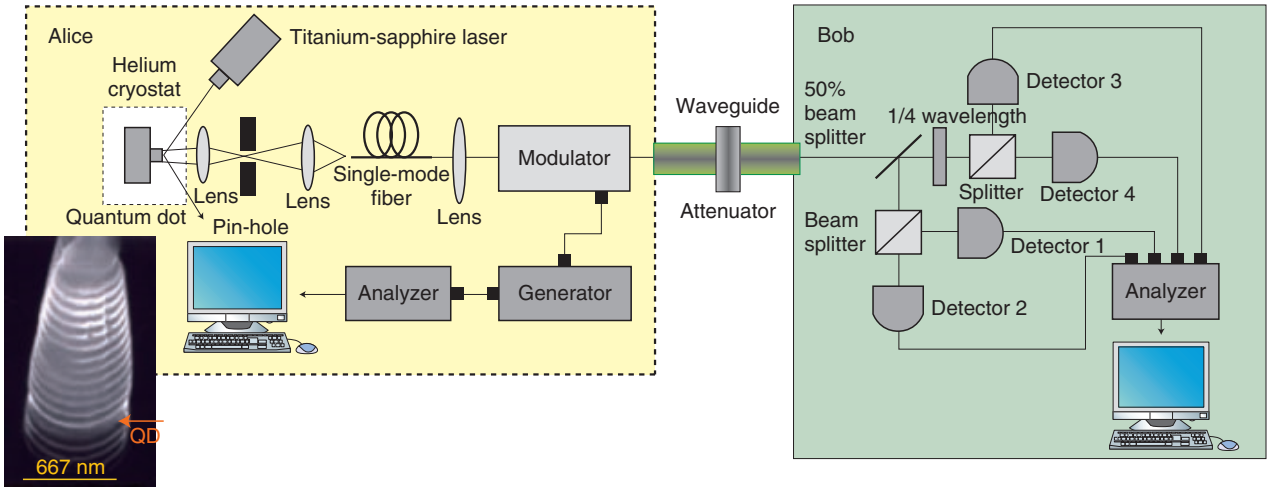


Fig. 3. BB84 QKD experimental setup using single-photon source.

QKD Network project [5], [6] in which NTT participated. The second candidate is to generate a secret key between a satellite and a ground base and then have the satellite swap the key with another ground base. In fact, such experiments are currently being prepared by the EU and Japan [7]. The third candidate is the quantum repeater, which is a future technology for repeating quantum information without converting it into classical information. This is considered to be the core technology for future QICT, as well as QKD, and is now being actively investigated all over the world [8].

3. NTT research and development (R&D)

NTT has been engaged in the basic research field of QICT: quantum optics. For QKD, theoretical investigation came first and experimental efforts started later, in 2000. Our collaboration with Professor Yoshihisa Yamamoto of Stanford University led to BB84 QKD experiments using a single-photon emitter with a quantum dot (wavelength: 0.8 μm) [9]. Single photons emitted from the quantum dot embedded in the pillar structure shown in the scanning electron micrograph, **Fig. 3** (left), are sent to Bob after being encoded in one of four polarization states (two logical bits × two bases). Bob measures the photons

by randomly choosing a basis using polarization beam splitters and four SPDs.

NTT and Stanford University proposed a new QKD protocol, Differential Phase Shift Quantum Key Distribution (DPS-QKD), in 2003 [10]. It applies a modern optical communication protocol, differential phase shift keying (DPSK) to the quantum regime. DPS-QKD uses a weak coherent state extending over multiple pulses, which is in clear contrast to the former QKD proposals that used quantum states of single photons, as shown at the bottom of Fig. 2. The DPS-QKD system is simple and applicable to a high clock rate and has good tolerance to the photon number splitting attack, which is an attack in which the number of photons in a pulse is counted and information is stolen by splitting one of the pulse's many photons. Moreover, in DPS-QKD, all the arriving photons can generate a key, whereas in BB84, half of them on average do not generate a key because of basis mismatch. A related protocol is the Coherent One-Way (COW) protocol [3]. NTT Basic Research Laboratories has used this DPS-QKD protocol and reported system experiments for clock rates from 1 GHz to 10 GHz.

NTT is also developing various improved SPDs. A conventional telecommunications wavelength SPD is the InGaAs avalanche photodiode (APD), which has the problems of low efficiency, high dark count rate, and limited slow gate-mode operation because of the after-pulse signal produced by the residual charges after photon detection. In contrast, the Si APD has a low dark count rate and does not need gate mode operation, but it is highly efficient only for photons with a relatively short wavelength. We have developed and verified a frequency-up-conversion SPD system by raising the photon frequency (making the wavelength shorter) by using periodically poled lithium nitride (PPLN) nonlinear-optics crystal and an intensive pump light and by detecting the photons with a Si-APD. We have also performed a QKD experiment that demonstrated a very high key generation rate with a fast hybrid single-photon detector and frequency up-conversion [11]. Recently, over-1-GHz clock operations have been demonstrated by improving the InGaAs-APD's optical signal analyzing circuit [12]. A superconducting single-photon detector (SSPD) has attracted much attention for its extremely small dark-count and high-speed operations. SSPD performance has been improving rapidly [13].

So far, we have discussed QKD with single photons or attenuated coherent light. It is known that quantum mechanics can allow an intriguing state of multi-quantum systems: the *quantum entangled state*. The technology for generating entangled photon pairs has matured; in particular, NTT has been leading telecommunications-band entangled photon-pair generation and its QKD applications [14]. In the future, we will pursue R&D of quantum repeaters and the connection of remote quantum computers to achieve highly developed quantum networking.

4. Prospects

From the perspective of the importance of privacy protection in the modern information society, the *unconditional security* of QKD seems appealing. However, the security of a system is not the sum of the securities of its components, but their product. For example, the total security is zero if the obtained secret keys are treated carelessly. In this sense, we could regard QKD R&D as a challenge toward ultimate security. Moreover, while previous R&D has been seeds- or hardware-oriented, more weight is expected to be given to applications and software in the future. QKD is an attractive subject with practical applications as well as a fundamental science.

Acknowledgment

Part of this research was done with the support of NICT and JST-CREST.

References

[1] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous Operation of High Bit Rate Quantum Key Distribution," Appl. Phys. Lett., Vol. 96, No. 16, p. 161102, 2010.

[2] H. Takesue, S. Woo Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum Key Distribution over a 40-dB Channel Loss Using Superconducting Single-photon Detectors," Nature Photonics, Vol. 1, No. 6, pp. 343–348, 2007.

[3] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High Rate, Long-distance Quantum Key Distribution over 250 km of Ultra Low Loss Fibres," New. J. Phys., Vol. 11, No. 075003, 2009.

[4] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New J. Phys., Vol. 11, No. 075001, 2009.

[5] http://www.uqcc2010.org/.

[6] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K.

Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger, "Field Test of Quantum Key Distribution in the Tokyo QKD Network," Opt. Express, Vol. 19, No. 11, pp. 10387–10409, 2011.
[7] http://www.quantum.at/quest
[8] For example, H. J. Kimble, "The Quantum Internet," Nature, Vol. 453, No. 7198, pp. 1023–1030, 2008.
[9] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, "Quantum Cryptography with a Photon Turnstile," Nature, Vol. 420, No. 6917, p. 762, 2002.
[10] Y. Tokura and T. Honjo, "Differential Phase Shift Quantum Key Distribution (DPS-QKD) Experiments," NTT Technical Review, Vol. 9, No. 9, 2011.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa8.html
[11] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, and Y. Yamamoto, "Megabits Secure Key Rate Quantum Key Distribution," New J. Phys., Vol. 11, p. 045010, 2009.
[12] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue, "High-rate Quantum Key Distribution over 100 km Using Ultra-low-noise, 2-GHz Sinusoidally Gated InGaAs/InP Avalanche Photodiodes," Opt. Express, Vol. 19, No. 11, pp. 10632–10639, 2011.
[13] H. Shibata, "Superconducting Single-photon Detectors," NTT Technical Review, Vol. 9, No. 9, 2011.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa9.html
[14] H. Takesue, "Quantum Communication Using Entangled Photon Pairs..Toward Quantum Repeaters," NTT Technical Review, Vol. 9, No. 9, 2011.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa10.html

Yasuhiro Tokura
Executive Manager, Optical Science Laboratory, NTT Basic Research Laboratories.
He received the B.S., M.S., and Ph.D. degrees from the University of Tokyo in 1983, 1985, and 1998, respectively. In 1985, he joined NTT Musashino Electrical Communications Laboratories, where he engaged in research on semiconductor nanoscience, quantum transport, and quantum information science. From 1998 to 1999, he was a visiting scientist in the Department of Applied Physics, Technical University of Delft, The Netherlands. Since 2004, he has been the group leader of the Quantum Optical State Control Research Group and a guest professor at Tokyo University of Science. Since 2010, he has also been a guest professor at the National Institute of Informatics.

Theory of the Security of Quantum Key Distribution

Kiyoshi Tamaki† *and Go Kato*

Abstract

We introduce the theory of the security of quantum key distribution, which features the fact that no one, including hackers, can break the laws of nature. By contrast, the security of conventional cryptography, which is widely used for communications, cannot be guaranteed even in principle.

1. Introduction

1.1 Quantum key distribution

Quantum cryptography, especially quantum key distribution (QKD), is a way to securely distribute a secret key to legitimate parties. Here, a *key* is a table of random numbers shared by legitimate users in such a way that the information is known only to them, and *secure* means secure against any possible eavesdropping, which is the highest level of security. In this article, we introduce the theory of the security of QKD and say a few words about practical security where we use practical devices.

1.2 One-time pad

What would you think if you received an email from a friend that read "rdlmgvmyroorlmbvm"? At first glance, it does not make sense and looks like a random alphabetic string. You might be worried that your friend's cell phone or personal computer is infected by a computer virus. If you are a good puzzle-solver, however, you would notice that this sentence actually does make sense. Instead of the message being typed directly, this sentence was processed (encrypted) to make it difficult to understand its message. The encryption method used here is uses complementary letters. For instance, to convey Z, you write A; for B, you write Y, and so on. Once you notice this rule, the sentence turns out to be "iwonbillionyen" meaning that your friend won a billion yen and wanted to tell you privately (the message to be conveyed is called plain text). This is a simple example, but it captures the essence of cryptography in the following senses.

(1) Someone who knows the encryption rule can immediately decrypt the message.
(2) Those who do not know the rule, for instance hackers or eavesdroppers, cannot immediately decrypt the message.

The former is the requirement that the sender and receiver communicate faithfully. In our example, the relationship among the words corresponds to this encryption rule, and an encrypted text can easily be decrypted by sharing this rule between the sender and receiver (hereinafter, we call this rule the key). The latter condition refers to the requirement that the communication between the sender and receiver must be secret and must be kept from eavesdroppers. It would be natural to define secure cryptography as a process that ensures an eavesdropper (usually called Eve) will take a long time to decrypt the message. In the case of an encryption method with a fixed key, however, it seems to be impossible to make Eve's decryption time very long. One of the most important points here is that some information, such as email address, header information, receiver's name, time information, etc., has already leaked to potential eavesdroppers in most communications. Thus, Eve can acquire information about the key by using this information together with the encrypted message, and it follows that the more the sender and receiver communicate, the more information about the key is leaked to Eve. Eventually, all the information about the key is known to her.

To resolve this problem, how about changing the

† NTT Basic Research Laboratories
Atsugi-shi, 243-0198 Japan

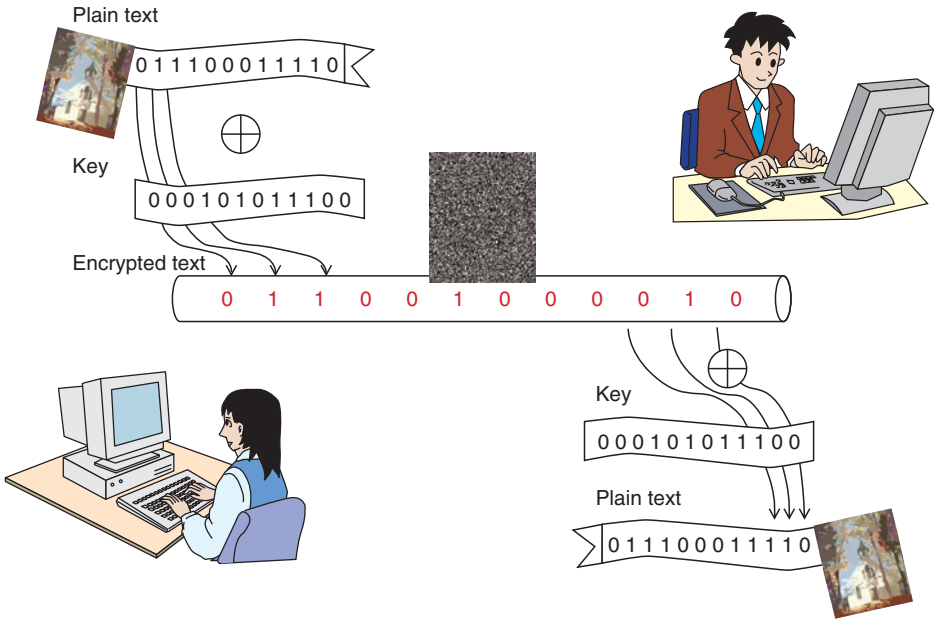


Fig. 1. Cryptographic communication using the key.

key every time we communicate, or even changing the key for each word? This approach does not protect information already known to Eve, but makes the already-known-information useless for obtaining the rest of the key information. This type of encryption method where different encryption methods are used for each message is called a one-time-pad, and it has the strongest security (**Fig. 1**).

It is very common for usual communications to encode the message into a bit string, so encryption is done by randomly choosing encoding methods where 0 is encoded as 0 (1 is encoded as 1) or where 0 is encoded as 1 (1 is encoded as 0). The former encoding method assigns the bit value 0 in the key, and the latter assigns the bit value 1 in the key. Thus, the key is a random bit string shared by the sender and receiver of the message. The important points for security are that the key length must be the same as the length of the bit string encoding the plain text and that we use each bit of the key only once. Consequently, the one-time pad satisfies the abovementioned condition (1), and as it is impossible for Eve to obtain information that was previously unknown to her, it also satisfies condition (2).

The rest of the question is how to distribute such a key without leakage of its information to Eve? If we want to distribute the key by means of telecommunications, then we have no alternative to using communication channels that are fully accessible to Eve. One assumption that we have to make is that the sender and receiver can authenticate each other (otherwise users might talk with Eve!), which can be achieved by using an authentication protocol, which is a form of classical cryptography. Once secure distribution has been successfully achieved, the one-time-pad becomes a very powerful form of cryptography. But secure key distribution seems to be an impossible task at first glance since Eve seems to be able to obtain all the information flowing over the channels. It turns out that the amount of information about the key that can be extracted by Eve can be made very small by making use of the strange properties possessed by dim light (hereinafter, called a single photon) and of post-selection, and that this asymmetry between Eve and the users in terms of key information does make secure key distribution possible. This key distribution technique is QKD. It is not a way of communicating directly, but a way of sharing the key to be used later to encrypt the plain text.

1.3 Quantum mechanics

In this section, we give a brief explanation of quantum mechanics, which is necessary to understand how QKD works. Roughly speaking, quantum mechanics is a set of principles describing the behavior of very small particles, such as atoms, electrons,

and photons. One of the principles tells us that a particle can be in multiple states that are mutually exclusive. For instance, a single particle can exist in many locations simultaneously, which seems very odd to us since we take it for granted that objects normally exist at a single location; a state of this kind is called a superposition state. Another principle in quantum mechanics says that if you observe the location of a particle in the superposition state, then the particle appears in a single location (this principle is called *wave function collapse*), and it is impossible to deterministically predict where it will appear: we can only determine the probability of the particle appearing at various different locations. Moreover, when more than one particle is in a superposition state at multiple locations, then the superposition states at some locations enhance each other while those at other locations decrease each other. This state behavior is the same as the interference of waves on the surface of water, and just as in the case of the interference of water surface waves, which is mathematically determined by *phase*, the superposition state also has phase. This property is called the *wave character of a particle*, and we can say that a particle behaves like a particle as well as like a wave.

One might ask why everyday macroscopic objects do not exist at multiple positions? The answer is that such a relatively big object is always under observation: its location is revealed by light incident on it or through collisions with other particles, such as molecules or dust, so it exists at only a single position. Here, we note that it does not matter whether or not anyone actually observes the object's location: what matters is the fact that the incident light or colliding particles/dust in principle contain information about the object's location, and this information is enough to cause the object's wave function to collapse.

2. QKD

2.1 QKD protocol

Now, we are ready for the explanation of how QKD protocol works. In this article, we explain differential phase shift QKD (DPS-QKD), which was proposed by NTT in collaboration with Stanford University. Here, protocol means a sequence of steps, and in the description of the protocol, we usually assume that the devices used by the sender and receiver operate as those mathematical models require. We will come back to the issue of using actual devices later on.

The protocol starts with the generation of a single photon in the superposition state of position 1, position 2, ..., position N. Since the speed of light in a communication channel such as an optical fiber is constant, this position information is equivalently transformed into time-slot information. Furthermore, we encode a random bit string (N-1 bits) of information as N-1 adjacent relative phase differences. More precisely, the bit value 0 (1) is encoded as the relative phase 0 (π).

The receiver performs a measurement that reads out the relative phase differences. This measurement can be implemented by using beam splitters, which are optical components, and a single-photon detector, which can detect a single photon. An important point here is that since the sender sends only a single photon, the detector receives at most one photon, so at most only one out of the N-1 bits of relative information can be read. As we have mentioned, no one, including the sender and receiver, can ever predict which relative phase information will be read out. Thus, to share the same bit value, the receiver informs the sender over a conventional communication channel, such as a regular telephone, which relative phase information out of the N-1 bits has been read out. Here, note that the receiver must not report the bit value itself. After the sender keeps only the corresponding phase information, the sender and receiver share an identical bit value, and, after many repetitions of above steps, they can share multiple bit values, which form the key.

2.2 Can one eavesdrop on key information?

Next, we consider whether it is possible for Eve to obtain information about the key. A possible form of eavesdropping is one where Eve conducts the same measurement as the receiver. With this measurement, she can successfully get to know about 1 bit of information. Since the sender sends only a single photon, however, she has no idea about the rest of the bit string information. Thus, she has trouble choosing the remaining N-2 bits of information when she sends a single photon to the receiver. Suppose that she chooses the N-2 bits of information randomly. If the receiver accidentally reads out bit information that Eve knows, then the Eve has been successful. However, since no one can ever have control over which time slot information will be read out, there is always some probability that the receiver will read out N-2 bits of unknown information. Moreover, one bit of information that the receiver accidentally reads out from among the N-2 bits will be different from the sender's bit information with probability of 50% (this error is called the bit error). It follows that many

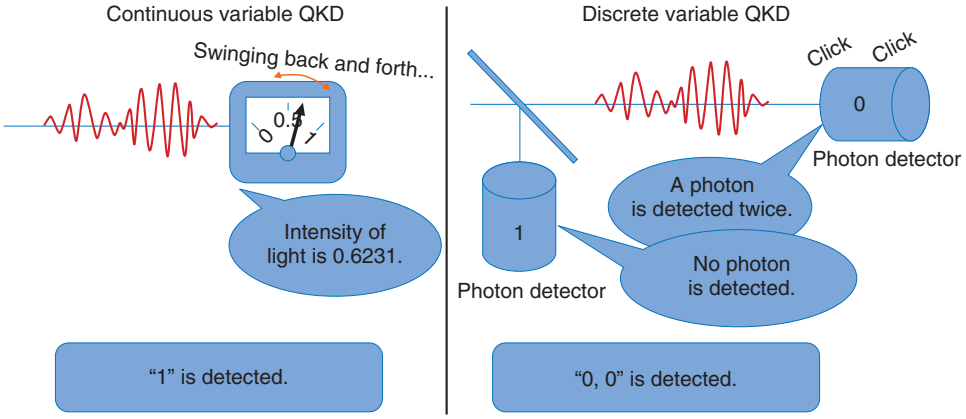


Fig. 2. Comparison of continuous and discrete variable QKDs.

repetitions of such communications makes the occurrence of bit errors very likely, which can be detected with high probability. More precisely, after many repetitions of one photon being sent by the sender and one bit information being received by the receiver, the sender and receiver agree by phone on randomly chosen sample bits among the bit data and check by phone whether they really match. If the bit error rate is below a certain value, then they accept all of the remaining bit data and proceed to data processing to distill the key over a public communication channel; otherwise, they discard all the remaining bit values. This threshold is determined from the theory of QKD, and it has been proven that the sender and receiver can generate a key if the bit error rate is below the threshold, regardless of Eve's eavesdropping strategy. This security does not assume any restrictions on the technologies that Eve may exploit. This highest level of security is called *unconditional security*.

2.3 Other types of QKD protocol

In this section, we briefly mention other types of QKD protocol. The QKD protocol that we have just described above assumes the use of a single-photon source, which it is known can be replaced by attenuated laser light without sacrificing the security. This kind of QKD protocol is called discrete variable QKD since the measurement outcome is bit information. On the other hand, a strong reference light or the difference in the output powers of the detectors can be used in another type of QKD protocol: continuous variable QKD (**Fig. 2**). Continuous variable QKD allows us to use efficient detectors that operate at normal temperatures, which is one advantage, but its security analysis is not as advanced as that for discrete variable QKD.

2.4 In what sense is QKD secure?

So far we have had a quick look at QKD. In this section, we would like to mention in what sense QKD is secure. As we have explained above, we can detect Eve's existence probabilistically, not deterministically, and we can never reduce to zero the probability of failing to detect Eve when she is present. For instance, the probability of the receiver detecting the relative phase information that Eve has extracted is very low if the number of detection events is large, but it still cannot be reduced to zero. In this sense, QKD cannot generate a key perfectly.

According to the theory of QKD, however, the probability of the actually generated key showing different properties, such as information leakage, from the perfect key can be made arbitrarily small by the users whatever form of eavesdropping was conducted by Eve. This should be okay since a very small probability should be fine in many communications. For instance, it would be realistic to set this probability to say 10^{-6}, which means that we would get a single bad event out of a million key generations. In the case of a perfect key with the length of a million bits, this number is 10^{-10^6}, which is an extremely small number and completely negligible. It corresponds to worrying about a single bad outcome in the lifetime of the universe. The fact that users can arbitrarily choose this failure probability is a very good point, and we use this probability to quantify key security in the QKD community.

Finally, we would like to mention the imperfections

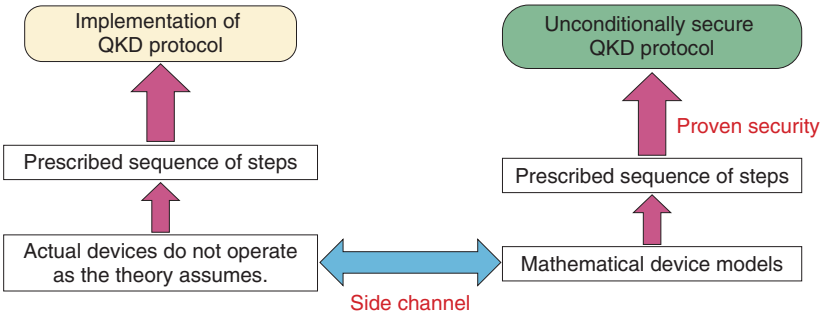
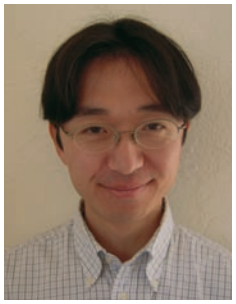


Fig. 3. Differences between protocol and its implementation.

of users' devices. In our discussion, users' devices were assumed to operate as required for the QKD protocol. However, actual devices do not necessarily operate as required; moreover, they may allow unwanted leakage of information. It is almost impossible to characterize all the details of all devices, so it follows that though such imperfections or unwanted information leakage may be made small through the development of technology or theory, they can never be eliminated. This kind of information leakage due to device imperfections is called a side channel and side channels exist in all types of communications (**Fig. 3**).

Some recent articles have reported a violation of QKD security, but we must note that this violation was done only by exploiting the side channel: one can never violate the QKD protocol itself. Moreover, the violation of QKD implementation by exploiting the side channel does not compromise the worth of QKD since the QKD protocol is at least unconditionally secure whereas no modern cryptographic protocol is. Therefore, in QKD research, we can concentrate our attention on the side channel. Further research on the QKD side channel is essential to achieve communication that is as secure as possible.

On the other hand, recent QKD systems can handle distances of only 50 km or at most 100 km and the key generation speed still needs to be improved: these are big disadvantages of QKD. Thus, we still need modern cryptography in many situations. Moreover, a side channel exists also in modern cryptography. Thus, collaboration between the QKD and modern-cryptography communities is very important to make the field of cryptography richer.



Kiyoshi Tamaki
Researcher, Quantum Optical State Control Research Group, NTT Basic Research Laboratories.
He received the M.Sc. degree and diploma in theoretical physics from Tokyo Institute of Technology in 1999 and 2001, respectively. From April 2001 to March 2004, he was a Ph.D. student supervised by Prof. Masato Koashi in Prof. Nobuyuki Imoto's group in the Graduate University for Advanced Studies (SOKENDAI), Japan. During his Ph.D. course, he visited Prof. Norbert Luetkenhaus's group at the University Erlangen-Nuremberg, Germany, for half a year. After receiving the Ph.D. degree, he worked at the Perimeter Institute for Theoretical Physics in Canada, under the support of Dr. Daniel Gottesman, and then worked as a postdoctoral fellow in Prof. Hoi-Kwong Lo's group at the University of Toronto, Canada. In January 2006, he joined the Quantum Optical State Control group in NTT Basic Research Laboratories. He is currently engaged in the theoretical study of quantum key distribution security. He is a member of the Physical Society of Japan (PSJ).

Go Kato
Researcher, Computing Theory Research Group, NTT Communication Science Laboratories.
He received the B.S., M.S., and Ph.D. degrees in science from the University of Tokyo in 1999, 2001, and 2004, respectively. He joined NTT Communication Science Laboratories in 2004 and has been studying quantum information theory. His research interests include the geometry of quantum states, entanglement, quantum cryptography, and quantum communication. He is a member of PSJ.

Differential Phase Shift Quantum Key Distribution (DPS-QKD) Experiments

Yasuhiro Tokura[†] *and Toshimori Honjo*

Abstract

NTT Basic Research Laboratories has been researching and developing differential phase shift quantum key distribution (DPS-QKD), a new QKD protocol. This article introduces the basics of this protocol, proof-of-principle experiments, the development of a prototype system, and a field experiment done at the Tokyo QKD Network demonstration in October 2010.

1. Differential phase shift quantum key distribution (DPS-QKD)

Quantum key distribution (QKD), which is a cryptosystem that uses the principles of quantum mechanics, has recently been attracting much attention as a way to achieve ultimate security in communication. In 2003, NTT and Stanford University jointly proposed differential phase shift quantum key distribution (DPS-QKD) [1], which uses the fact that only part of the relative phase information of attenuated light pulses can be read out. The setup and protocol of DPS-QKD are shown in **Fig. 1**.

First of all, the sender (called Alice) prepares a coherent pulse train and modulates the relative phase of the light pulses randomly with 0 or π. The light is then sent to the receiver (Bob) after being attenuated such that the number of photons per pulse is less than 1. Bob uses a one-pulse delay interferometer to cause successive pulses to interfere and measures the relative phase information with a set of photon detectors located at the interferometer's outputs. Since the source photon power is weak, only part of the relative phase information can be read out, but the obtained relative phase should be exactly the same as the phase modulations at the sender. Bob records the timestamp when a photon was detected and which of the detectors clicked (relative phase information itself). He then generates a key by assigning bit 0 to relative phase 0 and bit 1 to relative phase π. Bob then sends back to Alice only the timestamp information. Alice uses this information and her phase encoding records to generate a key, which is called the sifted key*. Finally, after error-correction and privacy-amplification processes, final secure keys are generated and used in cryptic communication.

2. Proof-of-principle experiments

We have demonstrated the principle of this protocol and evaluated the limits of the key distribution distances and key generation rates using real optical fibers. The experimental setup is shown in **Fig. 2**. Alice modulates the intensity of the light from a laser with a wavelength of 1551 nm to generate 1-GHz repetition pulses. Random phases 0 or π are encoded using a pulse pattern generator. After the light intensity has been adjusted to 0.2 photons per pulse on average, the pulses are sent into an optical fiber. Bob receives the light pulses from Alice and inputs them to a one-pulse delay interferometer and detects photons with the two single-photon detectors

† NTT Basic Research Laboratories
Atsugi-shi, 243-0198 Japan

* Sifted key: The sifted key is the initial raw key generated through photon transmission using a QKD protocol such as DPS-QKD or BB84. It has some errors due to system imperfections, so the final key is distilled through the error-correction and privacy-amplification processes.

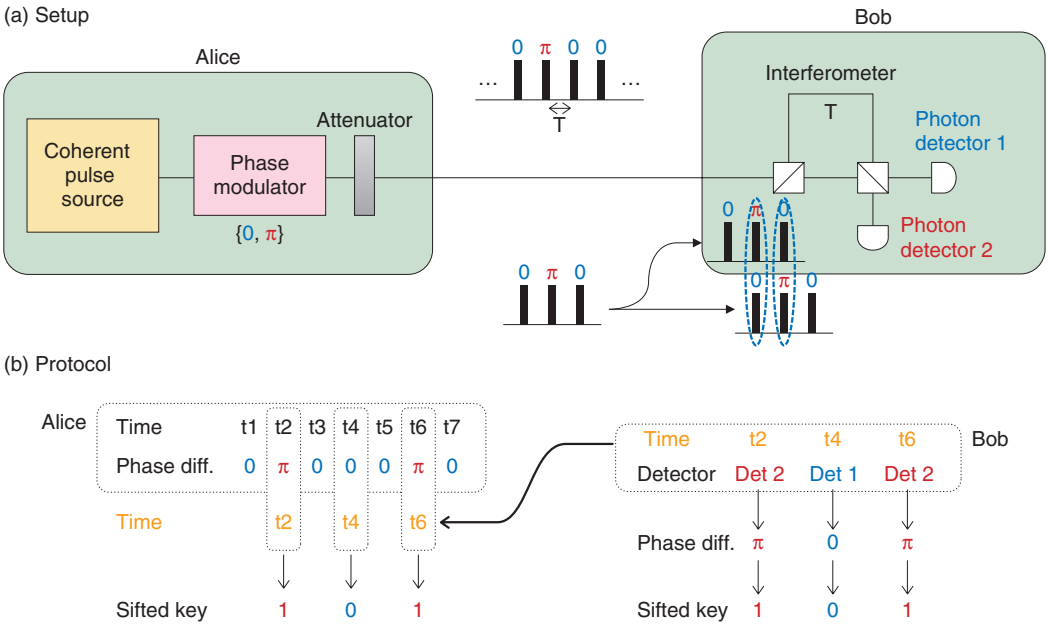


Fig. 1. Setup and protocol of DPS-QKD.

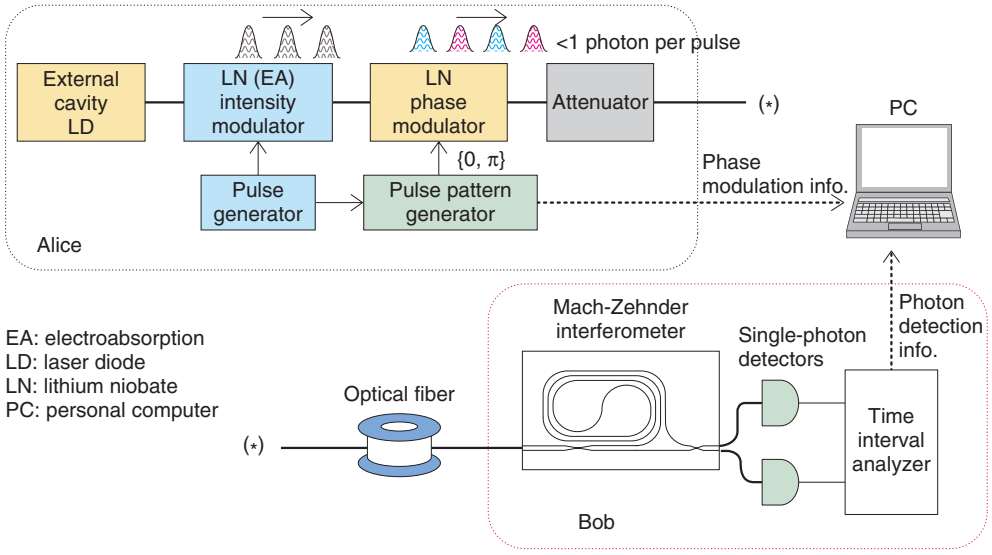


Fig. 2. Setup for the proof-of-principle experiments.

positioned at the interferometer's outputs. A time interval analyzer records the photon detection time and information about which of the detectors clicked. The sifted key is generated from this record by the abovementioned protocol, and the key generation rates and error rates are estimated.

The main issues so far have been the stability of the interferometer and the performance of the photon detectors. To obtain stable photon interference, we used a Mach-Zehnder interferometer (MZI) based on planar lightwave circuit (PLC) technology using quartz glass waveguides; this technology was developed by NTT. Since the optical path difference was ten times longer than that of conventional optical

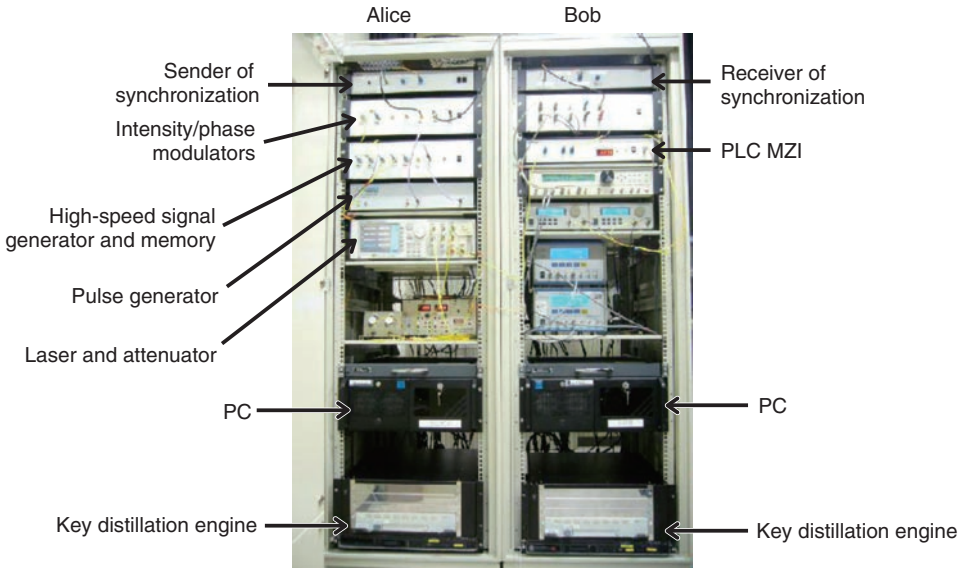


Fig. 3. Prototype system.

communications, stabilization had previously been a problem, but this PLC MZI showed an extinction ratio of more than 20 dB (corresponding to a bit error of less than 1%), which enabled us to perform a successful demonstration. As for the photon detectors, performance improvement accompanies the use of a longer key distribution length. The first demonstration in 2004 used an InGaAs avalanche photodiode (APD), and 100-km distribution was demonstrated using a photon detector system by converting long-wavelength photons to a shorter wavelength and detecting them with a fast, high-efficiency Si photon detector [2]. In 2007, we succeeded in achieving 200-km distribution with superconductor-based single-photon detectors, which enabled us to raise the repetition frequency to 10 GHz [3].

As shown in Fig. 1, this protocol requires huge random numbers. While a pseudo-random generator is usually used, a fast physical random generator is necessary to improve the security. Recently, a random generator with a generation rate of more than 1 Gbit/s using chaotic fluctuations of laser light has been developed and applied to DPS-QKD experiments [4].

3. Prototype system

DPS-QKD has been confirmed through several experiments, and we have started developing a prototype system. Its appearance is shown in **Fig. 3**. For the prototype implementation, we developed a high-speed signal generator and its memory unit using a field programmable gate array (FPGA). This is on Alice's side for generating signals to modulate the phase and for keeping them until the key generation stage. As in the proof-of-principle experiments, Alice modulates the intensity of the laser light to generate a 1-GHz pulse train and then modulates the relative phases depending on the phase signal from the FPGA board. After being attenuated, the pulses are sent to Bob. On Bob's side, the relative phases are detected with a PLC MZI and single-photon detectors, and the obtained signal is continuously retrieved by a time-interval analyzer and fed to a personal computer, where a sifted key is generated. At the same time, only the detection time is sent to Alice via a network. Alice extracts the phase information stored in the FPGA board according to Bob's detection times and generates a sifted key. Finally, the sifted keys on both sides are sent to the key distillation engine (developed by NEC), which executes error correction and privacy amplification and generates the final secret key for cryptic communication.

4. Field experiments

With our prototype system, we participated in a testbed network experiment called Tokyo QKD Network [5], led by the National Institute of Information and Communications Technology (NICT). The

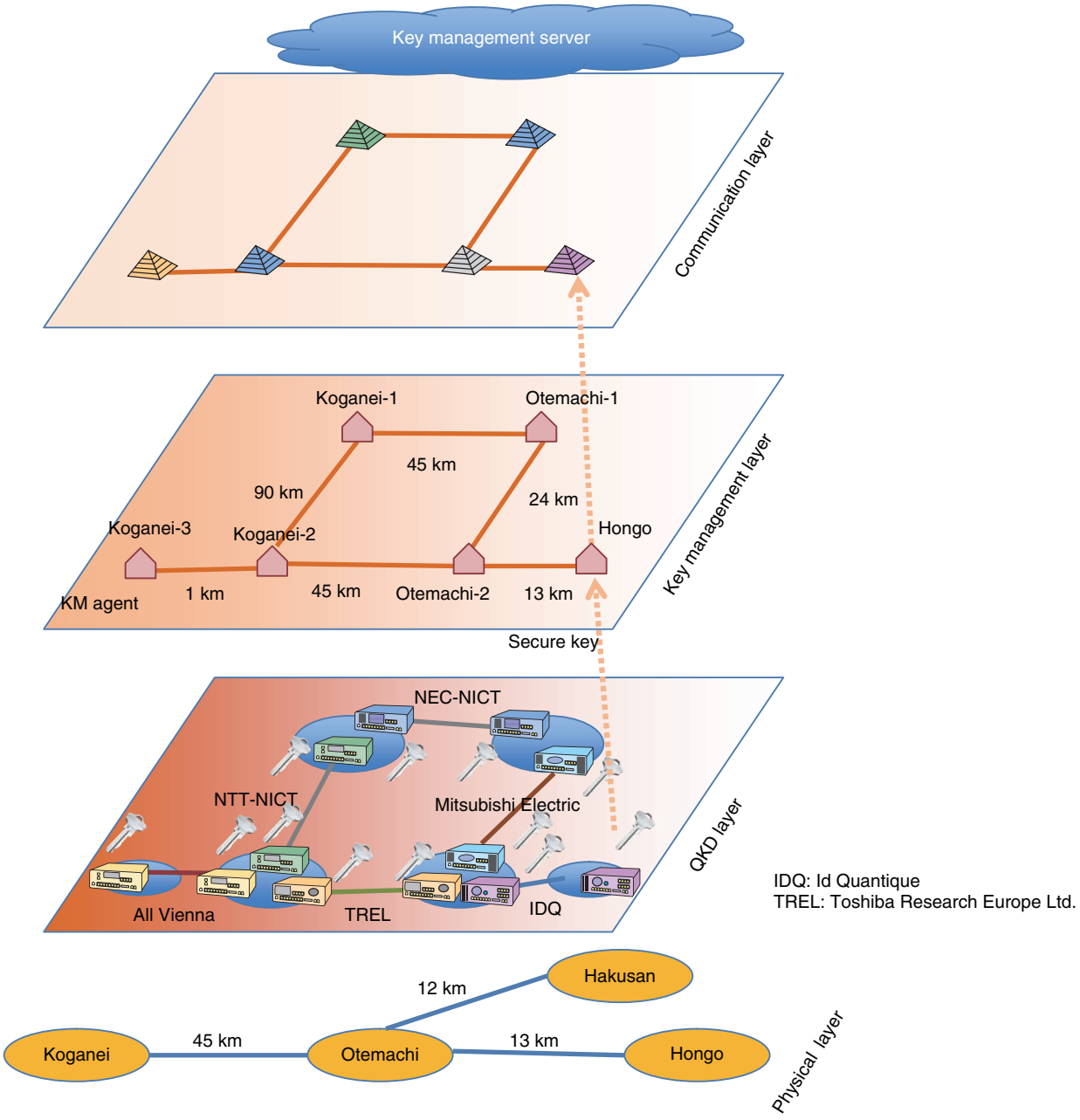


Fig. 4. Structure of Tokyo QKD network.

participants were NEC, Mitsubishi Electric, NTT supported by NICT, Toshiba Research Europe, Id Quantique (Geneva), and the All Vienna team. This QKD network was constructed using the testbed optical fiber network JGN2plus, connecting nodes at Otemachi, Koganei, Hakusan, and Hongo.

The network structure of this experiment is shown in **Fig. 4**. The transmission distances were Otemachi to Koganei: 45 km, Otemachi to Hakusan: 12 km, and Otemachi to Hongo: 13 km. There are many fibers in parallel on the Koganei-Otemachi, Otemachi-Hakusan, and Otemachi-Hongo routes and various network topologies are configured.

The lower layer, called the QKD layer, had six nodes; each team put its equipment at the nodes at both ends of a link. The QKD layer was constructed

over the physical layer. For example, NTT used 90 km of fiber between Koganei and Otemachi in a loopback configuration, NEC used 45 km of fiber between Koganei and Otemachi, Mitsubishi used 24 km of fiber between Otemachi and Hakusan in a loopback configuration, and ID Quantique used 13 km fiber between Otemachi and Hongo.

The secret key generated by QKD was supplied to the local key management agent and moved up to the key management layer. The key stored in the key management agent was used for cryptic communications such as a videoconference and voice communication. Between nodes that were not directly connected, the key was exchanged by being repeated at intermediate nodes.

NTT, in collaboration with NICT, was in charge of the longest loop-back segment used in the experiment (about 90 km). With the combination of our prototype system and the superconducting single-photon detectors developed by NICT, we were able to achieve stable key distribution. The stability test of sifted key generation was successfully run for about 8 days, with average generation rate of 18 kbit/s and average bit error rate of 2.2%. The stability test of final key generation including error correction and privacy amplification ran stably for about 4 hours, with a generation rate of 2.1 kbit/s. At an international conference (Updating Quantum Cryptography and Communications, UQCC) [6] in Oct. 2011, this QKD network demonstrated live detection of eavesdropping and subsequent automatic changeover to the redundant standby route, enabling an ultimately secure videoconference.

References

[1] K. Inoue, E. Waks, and Y. Yamamoto, "Differential Phase Shift Quantum Key Distribution Using Coherent Light," Phys. Rev. A, Vol. 68, No. 2, 022317, 2003.

[2] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, "100 km Differential Phase Shift Quantum Key Distribution Experiment with Low Jitter Up-conversion Detectors," Opt. Express, Vol. 14, No. 26, pp. 13073–13082, 2006.

[3] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum Key Distribution over a 40-dB Channel Loss Using Superconducting Single-photon Detectors," Nature Photonics, Vol. 1, No. 6, pp. 343–348, 2007.

[4] T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura, "Differential-phase-shift Quantum Key Distribution Experiment Using Fast Physical Random Bit Generator with Chaotic Semiconductor Lasers," Opt. Express, Vol. 17, No. 11, pp. 9053–9061, 2009.

[5] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger, "Field Test of Quantum Key Distribution in the Tokyo QKD Network," Opt. Express, Vol. 19, No. 11, pp. 10387–10409, 2011.

[6] http://www.uqcc2010.org/

Yasuhiro Tokura

Executive Manager, Optical Science Laboratory, NTT Basic Research Laboratories.

He received the B.S., M.S., and Ph.D. degrees from the University of Tokyo in 1983, 1985, and 1998, respectively. In 1985, he joined NTT Musashino Electrical Communications Laboratories, where he engaged in research on semiconductor nanoscience, quantum transport, and quantum information science. From 1998 to 1999, he was a visiting scientist in the Department of Applied Physics, Technical University of Delft, The Netherlands. Since 2004, he has been the group leader of the Quantum Optical State Control Research Group and a guest professor at Tokyo University of Science. Since 2010, he has also been a guest professor at the National Institute of Informatics.

Toshimori Honjo

Senior Research Engineer, Distributed Data Processing Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.S. degrees in information science from Tokyo Institute of Technology in 1996 and 1998 and the Ph.D. degree in engineering from Osaka University in 2007, respectively. In 1998, he joined NTT Software Laboratories, Musashino, where he engaged in research on the design and implementation of a network protocol stack in operating systems for secure mobile communications. From 2003 to 2010, he engaged in research on quantum optics and quantum key distribution at NTT Basic Research Laboratories. In 2009, he was a visiting researcher at the University of Vienna, Austria. Since 2010, he has been engaged in R&D of a large-scale distributed parallel data processing infrastructure. He moved to NTT Information Sharing Platform Laboratories in April 2011.

Superconducting Single-photon Detectors

Hiroyuki Shibata†

Abstract

This article describes the fabrication and properties of a single-photon detector made of a superconducting NbN nanowire. It also discusses suitable materials for future high-performance detectors and describes new fabrication processes for MgB_2 nanowire.

1. Introduction

Quantum cryptography is being intensively studied as a future optical network technology that assures the ultimate security in communications. In the standard optical communications network, one bit of information is represented by one optical pulse, which consists of more than 10,000 photons. In quantum cryptography, an extremely weak optical pulse consisting of less than one photon is used for one bit of information. It is impossible to amplify the optical pulse using an optical amplifier in a quantum cryptography network because quantum fluctuation, the essential feature of quantum cryptography, disappears with pulse amplification. The solution is to use high-performance single-photon detectors (SPDs) to increase the distance and speed of quantum cryptography communications. Many kinds of SPDs with different operating principles have been developed. Among them, SPDs made of a superconducting nanowire show the highest performance and are now used in many quantum cryptography experiments [1], [2].

2. Superconducting SPD

The superconducting single-photon detector (SSPD) developed by NTT Basic Research Laboratories [3] is shown in **Fig. 1**. In general, superconducting devices need to be cooled to a very low temperature, and the complexity and large size of the liquid-helium cooling equipment often limits the practical application of superconducting devices. However, NTT's detector is only 110 cm × 50 cm × 60 cm in size and can fit into a standard 19-inch-wide rack. It uses a cryocooler, so one can reach below 3 K by simply switching on the 100-V AC supply. The superconducting device is located at the middle of the cylinder shown in Fig. 1(a). As shown in Figs. 1(b) and (c), it is 10 μm square. The nanowire inside the device is 100 nm wide and 4 nm thick (Fig. 1(d)). The device is illuminated by extremely weak optical pulses through an optical fiber from outside the cylinder.

The mechanism of single-photon detection in the device is illustrated in Fig. 1(d). When electrical current flows in the superconducting nanowire, no voltage appears on the nanowire because the resistance is completely zero. When a single photon is absorbed at some point in the nanowire, the temperature at that point increases, superconductivity is locally destroyed, and the state at the point becomes normal (non-superconducting). If the nanowire is very narrow, the flowing current is completely protected by the normal state, and finite resistivity appears in the nanowire. Since the nanowire is being cooled by the cryocooler, its finite resistance rapidly disappears and it becomes superconducting again. These resistance changes create a voltage pulse, which is used to detect the arrival of a single photon at the superconducting nanowire. It may sound strange that only one photon can destroy superconductivity. However, while the superconducting energy gap of the

† NTT Basic Research Laboratories
Atsugi-shi, 243-0198 Japan

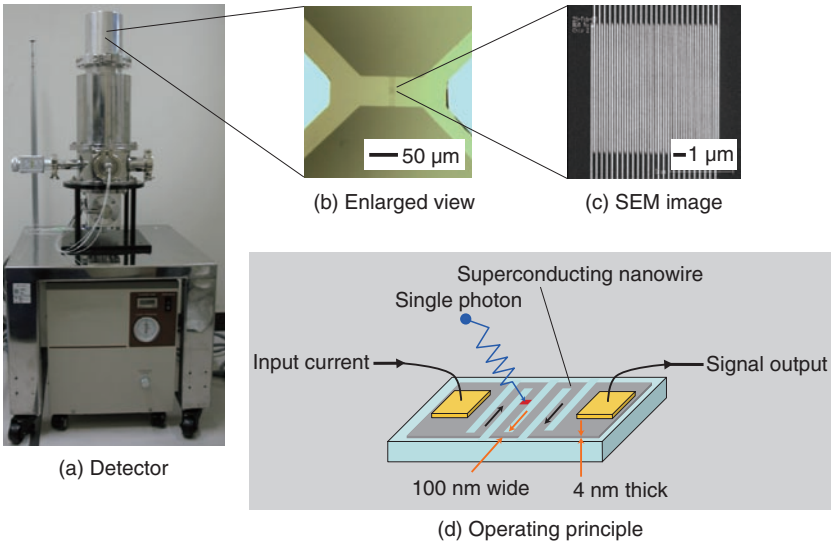


Fig. 1. Superconducting single-photon detector.

superconductor is a few millielectron volts, the energy of a single photon at a wavelength of 1.5 μm is 0.83 eV, which is high enough to destroy superconductivity locally. From the above device operating principle, it is clear that the nanowire must be narrow enough to protect the superconducting current completely. This is achieved by using superconductor nanofabrication as fine as 100 nm and growth of an ultrathin superconducting film with a thickness of 4 nm.

3. Superconducting materials

As the superconducting materials for the device, my colleagues and I used niobium (Nb) or niobium nitride (NbN) because they have well established nanofabrication and ultrathin film growth technologies. However, their transition temperatures (T_c) are relatively low among superconductors: 9 K for Nb and 16 K for NbN. Using a superconductor with a higher T_c would make it possible to operate the detector at a higher temperature, which would lead to further downsizing and energy savings.

The discovery year and T_c of several superconductors are summarized in **Fig. 2**. Cuprates and iron-based superconductors seem to be good candidates for detectors because they have higher T_c values. However, these materials are complex compounds with four or more elements, so it is quite difficult to use them to fabricate high-quality ultrathin films and narrow nanowires with today's technologies [4].

Magnesium diboride (MgB_2) has a T_c of 39 K. This is lower than that of cuprate and Fe-based superconductors, but the highest T_c among metallic and intermetallic compounds. MgB_2 has a simple crystal structure with only two elements. Furthermore, device fabrication with MgB_2 is not as difficult as that with cuprate and Fe-based superconductors. We can also expect faster operation with MgB_2 than with Nb or NbN.

Some physical superconducting parameters are listed in **Table 1**. The operating speed of an SSPD is governed by the inductance of the device and the electron-phonon relaxation time of the material. The inductance is determined by the device structure and by the material's magnetic penetration depth. For the same device structure, a device with a shallower magnetic penetration depth has a lower inductance and a faster response. On the other hand, a device with a shorter electron-phonon relaxation time has a faster response because it can rapidly return to the superconducting state again by emitting phonons. MgB_2 has a shallower magnetic penetration depth and shorter electron-phonon relaxation time than NbN, so a device made of MgB_2 operates faster than one made of NbN. The magnetic penetration depths of MgB_2 and Nb are almost the same, but MgB_2 has a much shorter electron-phonon relaxation time than Nb, so a

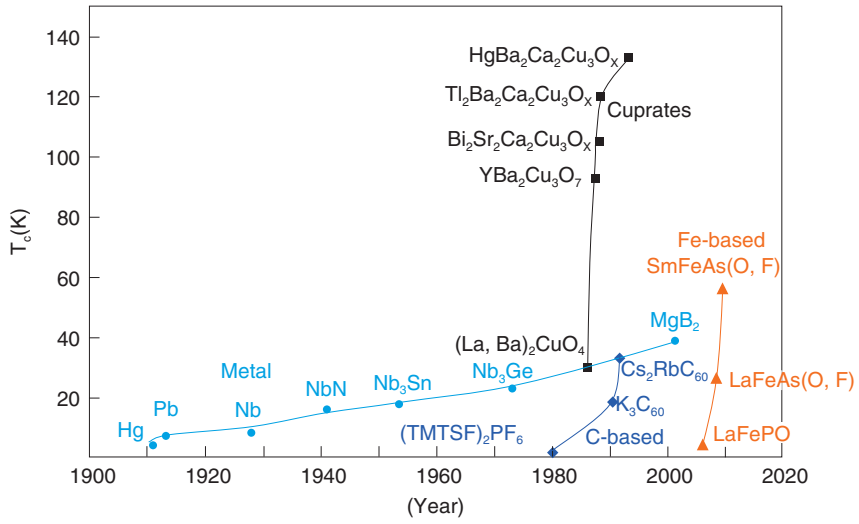


Fig. 2. T_c and discovery year of superconductors.

Table 1. Physical parameters of superconductors.

Material	T_c (K)	Magnetic penetration depth (nm)	Electron-phonon scattering time (ps)
Niobium (Nb)	9	39	370
Niobium nitride (NbN)	16	200	60
Magnesium diboride (MgB_2)	39	40	2
Cuprate ($YBa_2Cu_3O_7$)	92	200	1.1

device made of MgB_2 also works faster than one made of Nb. The magnetic penetration depth of MgB_2 is shallower than that of cuprate superconductors, but its electron-phonon relaxation time is longer. For devices with the same structure, one made of MgB_2 operates faster than one made of cuprates. However, a cuprate-based device with an optimized structure would work faster than an optimally structured MgB_2 device.

4. Fabrication of MgB_2 nanowire

Although MgB_2 seems to be a promising material for high-performance SSPDs, technologies for ultrathin film growth and nanofabrication of MgB_2 are not well established yet. We have succeeded in growing high-quality ultrathin MgB_2 film by using molecular beam epitaxy (MBE), which lets us precisely control the evaporation rates of B and Mg independently. We have also developed a new MgB_2 film nanofabrication technique.

The standard nanofabrication process for thin films is illustrated in **Fig. 3(a)**. The resist is spin-coated onto the film and patterned by electron beam lithography. Then the resist pattern is transferred to the thin film by etching. Finally, the resist is removed with an organic solvent and a nanopattern is obtained. The method can be applied to many kinds of materials if an appropriate etching gas is selected. It has been used to fabricate nanopatterns for many semiconductors including Nb and NbN. However, at present, it cannot be used for MgB_2 because no etching gas for MgB_2 has been found yet.

Our new MgB_2 film nanofabrication process is as follows (**Fig. 3(b)**). First, amorphous carbon is deposited on the substrate and resist is spin-coated onto the carbon film and patterned by electron beam lithography. Then the pattern is transferred to the amorphous carbon film by etching with a gas suitable for carbon (oxygen plasma). Next, the MgB_2 film is deposited on the amorphous pattern by MBE. Finally, the amorphous carbon nanostructure is lifted off and the MgB_2 nanopattern is obtained. The process is similar to the standard liftoff process using organic

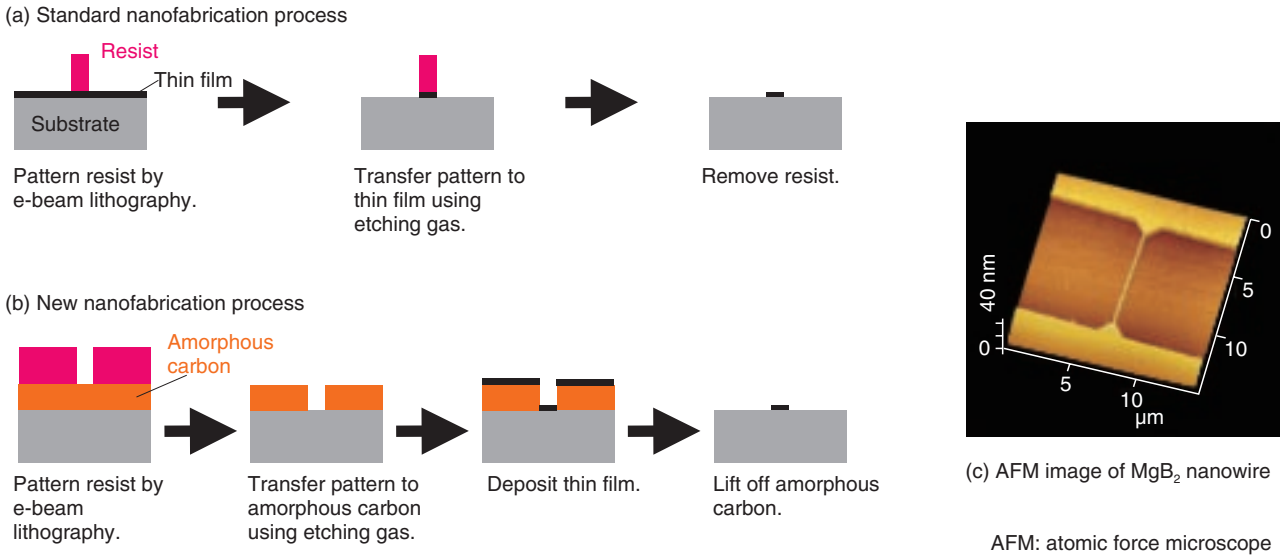


Fig. 3. Nanofabrication processes and MgB_2 nanowire.

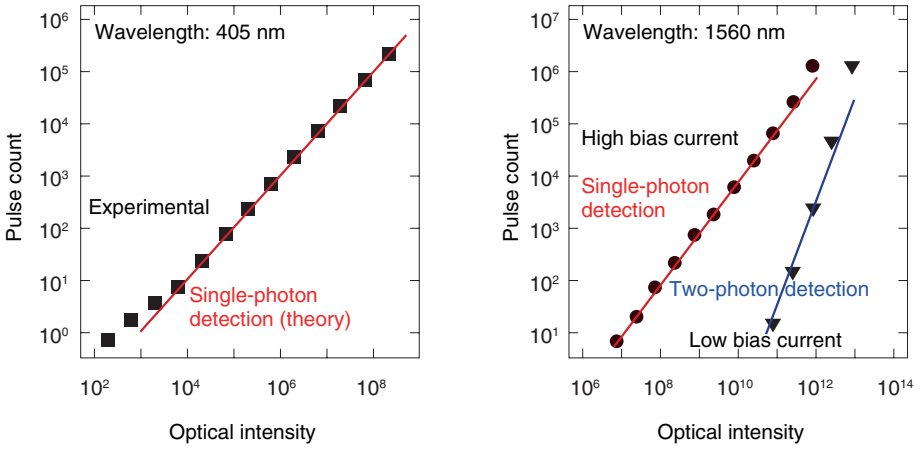


Fig. 4. Photon detection properties of MgB_2 nanowire.

resist. However, the standard liftoff process does not work for MgB_2 because the organic resist is destroyed by the high temperature used for MgB_2 growth. By using inorganic amorphous carbon, we can grow MgB_2 thin film at a high temperature without destroying the carbon nanopattern.

An atomic force microscopy image of an MgB_2 nanowire fabricated by our new method is shown in **Fig. 3(c)**. The nanowire is smooth and 100 nm wide, 4 nm thick, and 10 μm long. Measurements of the superconducting properties of several nanowires confirmed that the electrical properties are not degraded during the nanofabrication process.

5. Single-photon-detection capability of MgB_2 nanowire

The optical response of an MgB_2 nanowire at different wavelengths is shown in **Fig. 4**. It is known that the number of photons in one optical pulse from an extremely weak coherent light source can be represented by the Poisson distribution function. In this case, the probability of detecting one photon is proportional to the mean photon number, which is equal

to the optical intensity. Therefore, if the detector is capable of detecting a single photon, the number of electrical pulses from the detector should be proportional to the optical intensity. As shown in Fig. 4(a), this is indeed the case, which means that the detector can detect single photons having a wavelength of 405 nm. For a wavelength of 1560 nm, the number of electrical pulses is proportional to the square of the optical intensity in the low-bias region (Fig. 4(b)). This means that it is impossible to detect a single photon since the energy of a single 1560-nm photon is too weak. Therefore, two photons are necessary to generate an electrical pulse. In the high-bias region, on the other hand, the number of electrical pulses is proportional to the optical intensity, indicating that the MgB_2 nanowire can have single-photon-detection capability even at 1560 nm. From these results, we conclude that the MgB_2 nanowire has potential as a high-performance SPD.

6. Conclusion

The superconducting nanowire SPD that my colleagues and I have been using for quantum cryptography experiments is made of NbN. Toward practical quantum cryptography in future communications networks, we will continue to make efforts to improve the performance and reduce the energy consumption and size of detectors. A promising candidate for a high-performance SSPD is MgB_2 nanowire.

References

[1] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum Key Distribution over a 40-dB Channel Loss Using Superconducting Single-photon Detectors," Nature Photonics 1, pp. 343–348, 2007.

[2] T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, and Y. Yamamoto, "Long-distance Entanglement-based Quantum Key Distribution over Optical Fiber," Opt. Express, Vol. 16, No. 23, pp. 19118–19126, 2008.

[3] T. Seki, H. Shibata, H. Takesue, Y. Tokura, and N. Imoto, "Comparison of Timing Jitter between NbN Superconducting Single-photon Detector and Avalanche Photodiode," Physica C, Vol. 470, No. 20, pp. 1534–1537, 2010.

[4] H. Shibata, T. Takesue, T. Honjo, T. Akazaki, and Y. Tokura, "Single-photon Detection Using Magnesium Diboride Superconducting Nanowires," Appl. Phys. Lett., Vol. 97, No. 21, p. 212504, 2010.

Hiroyuki Shibata

Senior Research Scientist, Quantum Optical State Control Research Group, Optical Science Laboratory, NTT Basic Research Laboratories.

He received the B.S., M.S., and Ph.D. degrees in physics from Waseda University, Tokyo, in 1985, 1987, and 1997, respectively. In 1987, he joined NTT Basic Research Laboratories, where he has been working on the physics, material development, and device fabrication of superconductors. He was a visiting scientist at Max Planck Institute for Solid State Research in 2003. He has been a guest professor at Osaka University since 2008. He is a member of the Physical Society of Japan, the Japan Society of Applied Physics, and the Institute of Electronics, Information and Communication Engineers.

Quantum Communication Using Entangled Photon Pairs— Toward Quantum Repeaters

Hiroki Takesue†

Abstract

This article describes entangled photon pair generation and its application to quantum communication experiments with the aim of achieving quantum repeaters, which are necessary for global-scale quantum communication networks.

1. Introduction

In the quantum key distribution (QKD) system, whose security is based on the fact that one cannot copy a photon with an arbitrary quantum state, the key distribution distance is limited by the photon loss that occurs in the transmission medium (usually, optical fiber). In conventional optical communication systems, the transmission distance can be extended by using optical amplifiers; however, with QKD, optical amplification cannot be used to extend the distance. Therefore, the maximum key distribution distance over optical fiber in previous QKD experiments was limited to 200 km. Even if single-photon detectors are significantly improved, it is considered extremely difficult to achieve key distribution over more than 500 km of fiber. However, the distance can be increased by using entangled photon pairs. Moreover, entangled photon pairs are essential resources for building scalable quantum communication systems based on quantum repeaters.

2. Entangled photon pair generation in the telecommunication band

An entangled photon pair is a state in which two photons show a correlation that cannot be explained by classical theory [1]. For example, a polarization-entangled photon pair is a state in which the polarization state of each photon is not fixed, but the relationship between the polarization states of the two photons is predetermined. My colleagues and I have been studying time-bin entangled photon pairs, which are suitable for fiber transmission.

As the first step towards generating time-bin entangled photon pairs, we generate temporally correlated photon pairs by using spontaneous parametric processes. We input a pump light into a nonlinear medium with the 2nd- or 3rd-order nonlinear optical effect. If we use a 2nd-order nonlinear medium, a pump photon is annihilated and a photon pair is created through spontaneous parametric downconversion (SPDC). With a 3rd-order medium, two pump photons are annihilated and a photon pair is created by spontaneous four-wave mixing (SFWM). In both cases, two photons are always generated simultaneously, and we call these photons a *photon pair*. Hereinafter, one photon of the pair is called the *signal* and the other is called the *idler*.

To generate time-bin entangled photon pairs, we input coherent double pulses into a nonlinear medium as a pump. If the pump power is small and the probability that the two pulses will generate photon pairs simultaneously is very low, we can obtain a state consisting of the coherent superposition of the photon-pair state generated by the 1st pulse and that generated by the 2nd pulse. This state can be expressed as

$$|\Phi\rangle=(|1\rangle_s|1\rangle_i+|2\rangle_s|2\rangle_i)/\sqrt{2}\,, \quad (1)$$

† NTT Basic Research Laboratories
Atsugi-shi, 243-0198 Japan

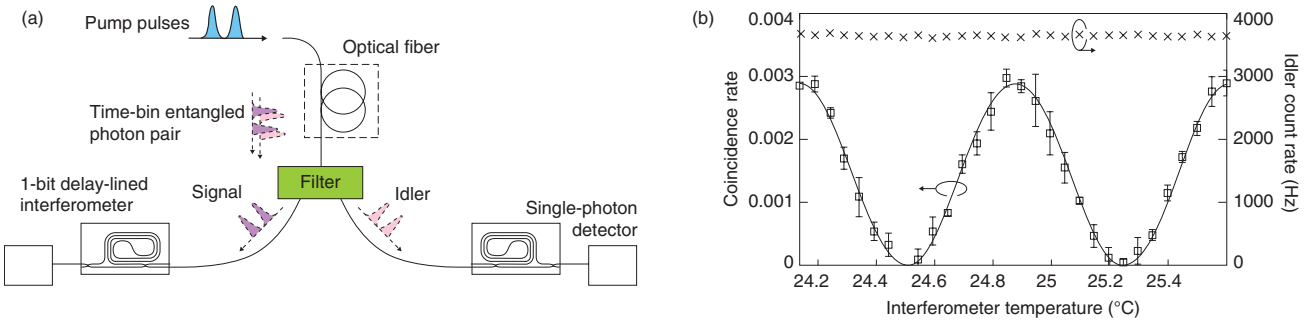


Fig. 1. Time-bin entanglement generation experiment. (a) Setup and (b) experimental results.

where $|X\rangle_y$ denotes a quantum state having a photon in the Xth time slot in mode y (s: signal, i: idler). This state shows a correlation in the measurement that distinguishes the photon's temporal position. Moreover, a correlation is also observed in a measurement that is nonorthogonal to the temporal measurement of the photon. One such measurement distinguishes whether a photon is a superposition of the $|1\rangle_y$ and $|2\rangle_y$ states with relative phase 0 $((|1\rangle_y+|2\rangle_y)/\sqrt{2})$ or π $((|1\rangle_y-|2\rangle_y)/\sqrt{2})$.

NTT has succeeded in generating 1.5-μm-band entangled photon pairs by SFWM in optical fibers [1], [2] and silicon wire waveguides [3] and by SPDC in periodically poled lithium niobate (PPLN) waveguides [4]. The setup for entanglement generation using optical fiber [2] is shown in **Fig. 1(a)**. We generated time-bin entangled photon pairs by SFWM in an optical fiber pumped by a double pulse whose temporal interval was 1 ns. The generated photons were separated into signal and idler photons by an optical filter. Then, each photon was launched into a 1-bit delay-line interferometer (an optical interferometer whose two optical paths have a length difference that corresponds to the temporal difference between two pulses). One of the output ports of each interferometer was connected to a single-photon detector. By adjusting the phase difference (ϕ_y) between the interferometer's two paths, we can achieve a measurement that detects a photon with quantum state $\frac{1}{\sqrt{2}}(|1\rangle_y+e^{-i\phi_y}|2\rangle_y)$. We used silica-waveguide-based interferometers in which the phase difference could be tuned by changing the substrate temperature. By measuring both photons in this way, we can investigate the correlation between photons in terms of phase difference. The experimental results are shown in **Fig. 1(b)**. Here, the × symbols denote the idler photon count rate when we swept the phase difference of the idler interferometer. We did not observe any significant variation in the idler count rate, which means that the phase difference was not predetermined. We then swept the phase difference of the idler interferometer while fixing that of the signal interferometer and measured the coincidence rate between two photons. The results are denoted by squares: they show a clear sinusoidal modulation. Thus, we experimentally confirmed the characteristic of entangled photon pairs: the state of each photon is not fixed but the relationship between two photons is predetermined.

3. QKD using entangled photon pairs

We can implement QKD using entangled photon pairs. We place an entangled photon pair source between two users (Alice and Bob). One photon from the pair is sent through an optical fiber to Alice and the other is similarly sent to Bob. Alice and Bob have instruments for performing two nonorthogonal measurements. They measure each photon with a measuring instrument chosen randomly from the two. With time-bin entangled photon pairs, we can use a *time measurement* that discriminates state $|1\rangle_y$ from state $|2\rangle_y$ and a *phase measurement* to distinguish $(|1\rangle_y+|2\rangle_y)/\sqrt{2}$ from $(|1\rangle_y-|2\rangle_y)/\sqrt{2}$ as the two nonorthogonal measurements. These measurements are implemented by using a 1-bit delay-line interferometer and two single-photon detectors that are connected to the output ports of the interferometer. In collaboration with the National Institute of Standards and Technology (NIST), Stanford University, and the National Institute of Information and Communications Technology (NICT), NTT has successfully performed a long-distance QKD experiment using time-bin entangled photon pairs [5]. We used a

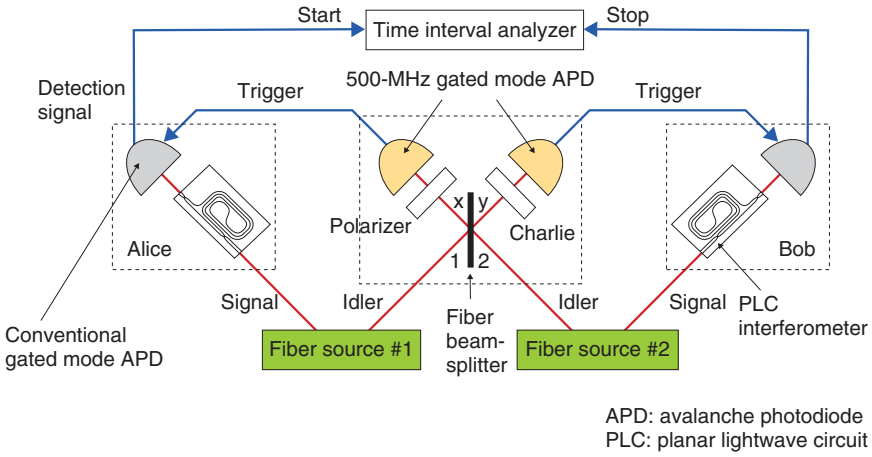


Fig. 2. Setup for entanglement swapping experiment.

high-purity time-bin entangled photon pair source based on a PPLN waveguide and superconducting single-photon detectors and achieved secure quantum key distribution over 100 km of fiber.

4. Towards quantum networking: entanglement swapping experiment

In theory, by using an entanglement-based QKD scheme, we can roughly double the key distribution distance compared with that obtained with conventional QKD without entangled photons. However, the distance is still limited by the photon loss caused by the transmission fiber. It is considered difficult to achieve a key distribution distance exceeding 1000 km using current optical fibers as the transmission medium. A quantum repeater is expected to overcome this distance limitation. One key technique for a quantum repeater is entanglement swapping. In this section, I describe an entanglement swapping experiment that was undertaken in the 1.5-μm telecommunications band [6].

The experimental setup, which is shown in **Fig. 2**, includes two entanglement sources, an intermediate node between the sources (referred to as Charlie), and two users: Alice and Bob. The entanglement sources are based on SFWM in optical fibers pumped by a 500-MHz pump pulse train. These sources generate sequential time-bin entangled photon pairs, whose quantum state is given by

$$|\mathrm{S}\rangle \rightarrow \frac{1}{N}\left(\sum_{j=1}^{N}|j\rangle_{1s}|j\rangle_{1i}\right)\otimes\left(\sum_{k=1}^{N}|k\rangle_{1s}|k\rangle_{1i}\right). \quad (2)$$

Here, subscripts 1 and 2 indicate that the states originated from sources 1 and 2, respectively. As shown in Fig. 2, the idler photons from the two sources were sent to Charlie through optical fibers, while the signal photons from source 1 (2) were sent to Alice (Bob). Alice, Bob, and Charlie performed coincidence measurements on the kth and $(k+1)$th time slots, where k is a natural number between 1 and N. The state of the two idler photons was therefore a mixed state composed of the following four states.

$$\begin{aligned}|\Phi_k^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|k\rangle_{1i}|k\rangle_{2i} \pm |k+1\rangle_{1i}|k+1\rangle_{2i})\\ |\Psi_k^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|k\rangle_{1i}|k+1\rangle_{2i} \pm |k+1\rangle_{1i}|k\rangle_{2i})\end{aligned} \quad (3)$$

These four are all maximally entangled states known as Bell states. We can transform Eq. (2) by using these four Bell states to

$$\begin{aligned}|\mathrm{S}\rangle \rightarrow \frac{1}{N\sqrt{2}}\Bigg\{&\sum_{k=1}^{N}|k\rangle_{1s}|k\rangle_{2s}(|\Phi_k^{+}\rangle + |\Phi_k^{-}\rangle)\\ &+\sum_{k=1}^{N-1}\Big[(|k\rangle_{1s}|k+1\rangle_{2s} + |k+1\rangle_{1s}|k\rangle_{2s})|\Psi_k^{+}\rangle +\\ &(|k\rangle_{1s}|k+1\rangle_{2s} - |k+1\rangle_{1s}|k\rangle_{2s})|\Psi_k^{-}\rangle\Big]\Bigg\}\end{aligned} \quad . \quad (4)$$

Here, terms that do not contribute to the coincidence measurement between the kth and $(k+1)$th slots are omitted for simplicity.

The idler photons that arrived at Charlie were input into a fiber coupler having two input/output ports. The idler photon from source 1 (2) was input into port 1 (2) of the coupler, and the two output ports were denoted ports x and y. These ports were connected to

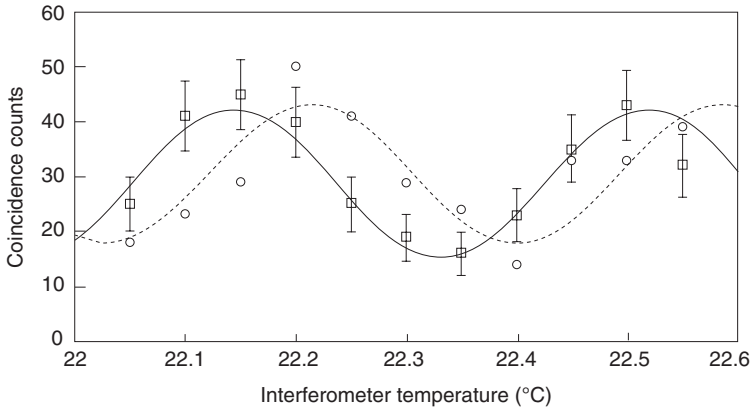


Fig. 3. Results of entanglement swapping.

single-photon detectors whose gate frequency was as high as 500 MHz. With current technologies, there is no way to distinguish which of the four Bell states the two incoming idler photons were in. However, it is relatively easy to implement a measurement to show that the incoming state was $|\Psi_k^-\rangle$ by using a fiber coupler followed by two single-photon detectors. It can be shown that the incoming photons were in the $|\Psi_k^-$ state if the two idler photons were output from different ports of the coupler and both were counted by the detectors. According to Eq. (5), the state of the two signal photons sent to Alice and Bob is projected to an entangled state $(|k\rangle_{1s}|k+1\rangle_{2s}-|k+1\rangle_{1s}|k\rangle_{2s})/\sqrt{2}$. Thus, by extracting events where two idler photons were observed to be in the Bell state $|\Psi_k^-\rangle$, we can *entangle* the two signal photons generated in two independent fibers that were originally uncorrelated. This procedure is called entanglement swapping.

We performed coincidence measurements similar to the one described in section 2 under the condition that the two idler photons were measured as being in the $|\Psi_k^-\rangle$ state at Charlie. The results are shown in **Fig. 3**. As we swept the temperature of Bob's interferometer, we observed a clear sinusoidal modulation in the coincidence counts. Thus, we confirmed that two signal photons generated in two independent sources were entangled.

To date, we have achieved only one-stage entanglement swapping using two sources. As a natural extension, we will try to achieve multistage entanglement swapping using three or more sources. In this way, we should be able to significantly extend the entanglement distribution distance.

5. Future work

By implementing QKD using an entangled state distributed by entanglement swapping, we can, in theory, extend the key distribution distance. However, in reality, since the probability of generating a photon pair at each source is not 100%, the probability of successful entanglement swapping decreases exponentially if we perform multistage entanglement swapping. Therefore, although it is theoretically possible to extend the entanglement distribution distance, the entanglement generation rate may be very small. Consequently, it is very difficult to construct a useful QKD system based on simple entanglement swapping.

We can solve this problem by using a *quantum memory* that stores the quantum state of light. A quantum memory is a device in which the quantum state of a photon is transferred to another quantum system such as an atom. Then, after the state has been stored for a while, we can convert it back to a photon state at an arbitrary time. This technique should let us improve the success probability of multistage entanglement swapping in the following way. When we succeed in entanglement swapping at a link, we store the entangled photons in quantum memories placed at the link's edge until an entanglement is generated at the adjacent links by entanglement swapping. Then, we convert the photons in the adjacent memories back to photons that engage in another round of entanglement swapping. Thus, we can avoid the exponential decay of the entanglement generation rate. This quantum communication scheme based on entanglement swapping using entangled states stored

in quantum memories is called a quantum repeater, and it is expected to be an essential scheme for achieving global-scale quantum communication. Many institutions, including NTT, are currently undertaking research aimed at achieving quantum repeaters.

References

[1] H. Takesue, "Generation of Polarization-entangled Photon Pairs in 1.5-μm Telecommunication Band," NTT Technical Review, Vol. 3, No. 12, pp. 52–60, 2005.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200512052.pdf

[2] H. Takesue and K. Inoue, "Generation of 1.5-μm Band Time-bin Entanglement Using Spontaneous Fiber Four-wave Mixing and Planar Lightwave Circuit Interferometers," Phys. Rev. A, Vol. 72, No. 4, p. 041804, 2005.

[3] H. Takesue, K. Harada, Y. Tokura, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, and S. Itabashi, "Entanglement Generation Using Silicon Wire Waveguide," NTT Technical Review Vol. 8, No. 2, 2010.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201002sf6.html

[4] H. Takesue, K. Inoue, O. Tadanaga, Y. Nishida, and M. Asobe, "Generation of Pulsed Polarization-entangled Photon Pairs in a 1.55-μm Band with a Periodically Poled Lithium Niobate Waveguide and an Orthogonal Polarization Delay Circuit," Opt. Lett., Vol. 30, No. 3, pp. 293–295, 2005.

[5] T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, and Y. Yamamoto, "Long-distance Entanglement-based Quantum Key Distribution over Optical Fiber," Opt. Express, Vol. 16, No. 23, pp. 19118–19126, 2008.

[6] H. Takesue and B. Miquel, "Entanglement Swapping Using Telecom-band Photons Generated in Fibers," Opt. Express, Vol. 17, No. 13, pp. 10748–10756, 2009.

Hiroki Takesue

Senior Research Scientist, Quantum Optical State Control Research Group, NTT Basic Research Laboratories.

He received the B.E., M.E., and Ph.D. degrees in engineering science from Osaka University in 1994, 1996, and 2002, respectively. He joined NTT in 1996, where he engaged in research on lightwave frequency synthesis, optical access networks using wavelength division multiplexing, and quantum communication. From 2004 to 2005, he was a Visiting Scholar at Stanford University, California, USA. He is a member of IEEE and the Japan Society of Applied Physics.

Activities and Status of Focus Group on Smart Grid in ITU-T

Tsuyoshi Masuo†

Abstract

This article describes the current status of the Focus Group on Smart Grid, which was established by ITU-T (International Telecommunication Union, Telecommunication Standardization Sector) in 2010, as initial study activities related to the Smart Grid, especially from the perspective of information and communications technology (ICT).

1. Introduction

The Smart Grid is a new electricity network that highly integrates advanced sensing and measurement technologies, information and communications technologies (ICTs), analytical and decision-making technologies, and automatic control technologies with energy and power technologies and the electricity grid infrastructure*. With energy and environmental issues becoming more important recently, various efforts related to the Smart Grid are being conducted around the world.

The establishment of the Focus Group on Smart Grid (FG Smart) [1] was officially approved in the ITU-T TSAG (International Telecommunication Union, Telecommunication Standardization Sector, Telecommunication Standardization Advisory Group) meeting held in February 2010 [2]. It followed on from discussions at an earlier meeting—the first ITU-T CTO (Chief Technology Officer) group meeting held in October 2009—about ITU-T's role in the field of smart grids as a hot topic of ICT. Because the technical area covered by smart grids is very wide ranging, FG Smart was established under TSAG to deal with issues related to multiple ITU-T Study Groups (SGs). Incidentally, the February 2010 TSAG meeting also officially approved the establishment of FG Cloud (Focus Group on Cloud Computing).

2. Management structure

After the February 2010 TSAG meeting, the Chairman and Vice-Chairman of FG Smart were nominated and approved by April 2010, and the first meeting of FG Smart was held in June 2010 in Geneva under a management structure consisting of one chairman (Germany) and three vice-chairmen (China, Japan, and Korea). Furthermore, in this first meeting, another vice-chairman from NIST (National Institute of Standards and Technology), which has had a lot of achievements in the smart grid area, was proposed by the chairman and approved. As a result, the management structure currently consists of one chairman and four vice-chairmen.

3. Activities

FG Smart has held seven official meetings to date. Its initial period was one year, so the seventh meeting held in June 2011 on Jeju Island, Korea, would have been the last one; however, the February 2011 TSAG meeting approved a half-year extension to enhance the output documents and promote collaboration with other standardization bodies. The meetings that have been held and are currently scheduled are listed in **Table 1**.

In the first FG Smart meeting, standardization development organizations (SDOs) and industry

† NTT Energy and Environment Laboratories
Musashino-shi, 180-8585 Japan

* The definition of Smart Grid is currently under discussion at ITU-T FG Smart.

Table 1. Meetings of FG Smart.

	Date	Place	Notes
1st	June 14–16, 2010	Geneva, Switzerland	
2nd	August 2–5, 2010	Geneva, Switzerland	Establishment of three WGs
3rd	October 11–15, 2010	Geneva, Switzerland	
4th	November 29 to December 3, 2010	Chicago, USA	Joint with SGIP/Grid-Interop2010
5th	January 10–14, 2011	Yokohama, Japan	Workshop and tours to experimental project in Japan
6th	April 4–8, 2011	Sophia Antipolis, France	Joint with ETSI Workshop on Smart Grid
7th	June 9–15, 2011	Jeju Island, Korea	
8th	August 22–26, 2011	Geneva, Switzerland	
9th	December 18–22, 2011	Geneva, Switzerland	Final meeting

groups such as NIST, ETSI (European Telecommunications Standards Institute), IEC (International Electrotechnical Commission), IEEE (Institute of Electrical and Electronic Engineers) and ZigBee Alliance introduced contribution documents that described their activities and outcomes. Participants discussed the target of FG Smart and methods of investigation, for example, the advantages and disadvantages of a vertical approach to studying each application related to smart grids and a horizontal approach to studying common issues such as smart grid architecture and requirements. As a result of this discussion, the second FG Smart meeting (August 2010), approved the establishment of three Working Groups (WGs): the Use Cases WG, Requirements WG, and Architecture WG. Each WG will create an output document called a Deliverable. In addition, it was agreed that a Terminology deliverable would also be created as a common activity among these three WGs. Since then, FG Smart has mainly conducted studies on the basis of contribution documents that proposed input texts for each deliverable in the corresponding WG meeting; in practice, however, the WG meetings have been held sequentially during the FG Smart meeting so that all FG Smart meeting participants could discuss and study all of the deliverables. The WG structure and the deliverables are listed in **Table 2**.

The fourth FG Smart meeting in Chicago, USA, and the sixth meeting in Sophia Antipolis, France, were held jointly with other conferences relevant to smart grids at the same locations in order to enhance interaction among participants of both. This is one of the features of FG activities: they are usually disclosed to even non-ITU-T sector members.

The fifth meeting was held in Yokohama, Japan, hosted by Mitsubishi Electric. In addition to the regular meetings, a workshop conference and tours to a smart house experimental project in the Minato-Mirai area of Yokohama supported by the Japanese Ministry of Internal Affairs and Communications (MIC) were provided to highlight Japan's efforts in the smart grid area.

Table 2. Structure of WGs and Deliverables.

	Output documents (Deliverables)
WG1	Use Cases
WG2	Requirements
WG3	Architecture
Ad hoc	Terminology
Plenary	Overview

4. Overview of studies

In the Use Cases WG's study activities, NIST's knowledge base called IKB (Interoperability Knowledge Base) [3], which was derived through its significant efforts, is considered to be a very important and useful information source. The high-level use-case categories currently proposed on the basis of IKB and input contribution documents to the Use Cases WG are listed in **Table 3**. For each category, detailed and specific use cases are being organized in a table format that includes items such as Actors, Domains, and Exchange Information. So far, many use cases, especially ones corresponding to AMI (Advanced Metering Infrastructure), Existing User's Screens, Managing Applications through/by Energy G/W (gateway), and Electric Vehicle, have been proposed. For example, in the case of Existing User's Screens, many use cases about systems for visualizing energy consumption in houses have been proposed.

In the Requirements WG and Architecture WG, as study activities progress, a new issue has arisen: the contents and scope of each deliverable should be

clarified and organized. To deal with this issue, the fourth meeting in Chicago approved the creation of a new Overview deliverable describing the basic concept of smart grids, goal of FG Smart, relationship with other SDOs, architecture overview from an ICT perspective, and so on.

The conceptual model of smart grids in this Overview deliverable refers to NIST's seven-domain model already incorporated in the activities of various SDOs. The Architecture overview is based on the three-layer (Service/Application, Network, and Energy) model proposed by ETSI with some modifications for the ICT perspective (**Figs. 1** and **2**).

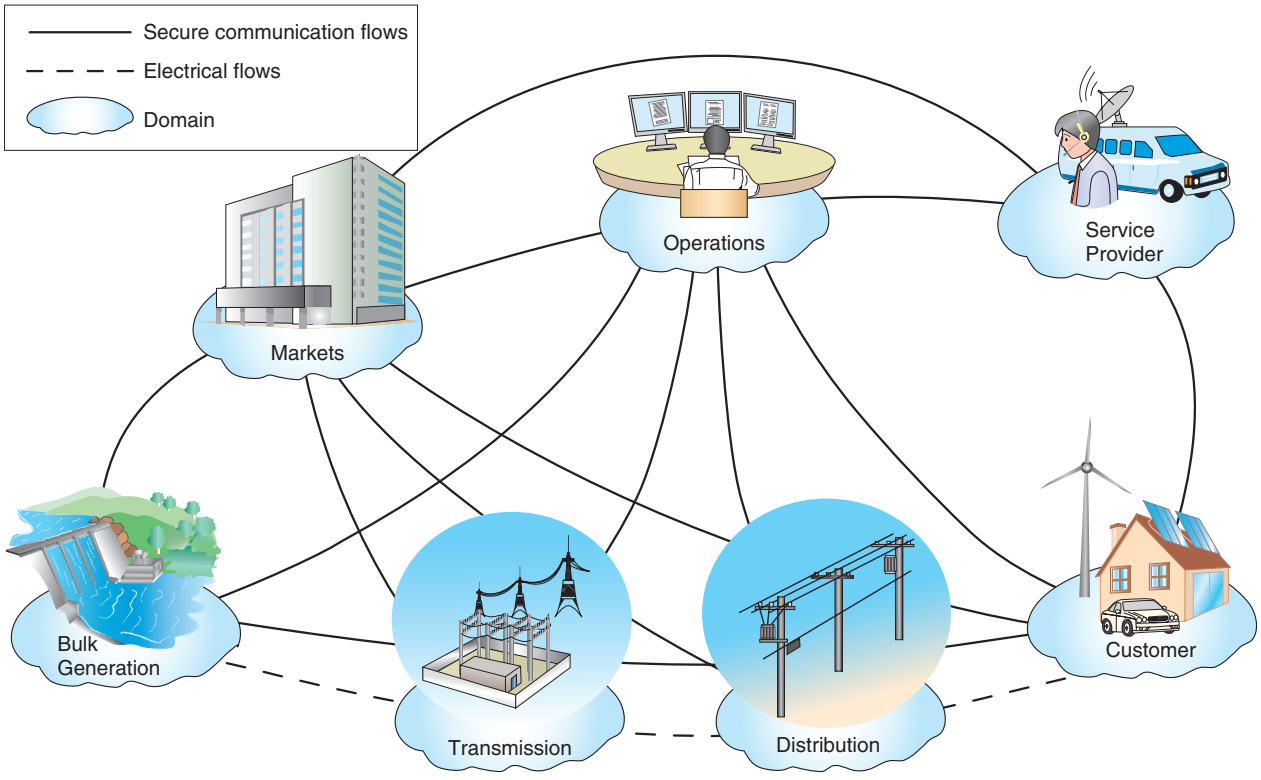
Currently, the Requirements and Architecture deliverables are being created in the manner of a breakdown Overview deliverable. In the case of the Architecture deliverable, a functional architecture model the same as the IPTV (Internet protocol television) architecture has been introduced (**Fig. 3**).

Table 3. High-level categories of use cases.

No	Title
1	Demand Response
2	WASA (Wide-Area Situational Awareness)
3	Energy Storage
4	Electric Transportation
5	AMI (Advanced Metering Infrastructure) systems
6	Distribution Grid Management
7	Market Operations
8	Existing User's Screens
9	Managing Appliances through/by Energy G/W
10	Electric Vehicle
11	Local Energy Generation/Injection

5. Future plans

Although the period of FG Smart has been extended to December 2011, all the deliverables will be sent to related SGs in ITU-T and other SDOs as liaison documents at the end of the eighth FG Smart meeting in August 2011. After that, with some feedback from



NIST Smart Grid Framework 1.0, January 2010.

Fig. 1. Conceptual domain model of Smart Grid by NIST.

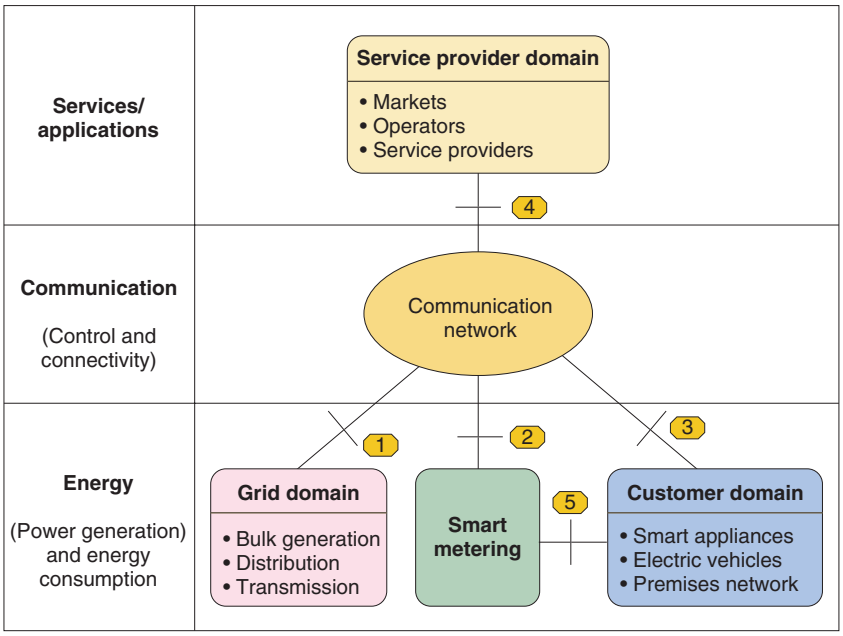


Fig. 2. Three-layer architecture model simplified with ICT perspective.

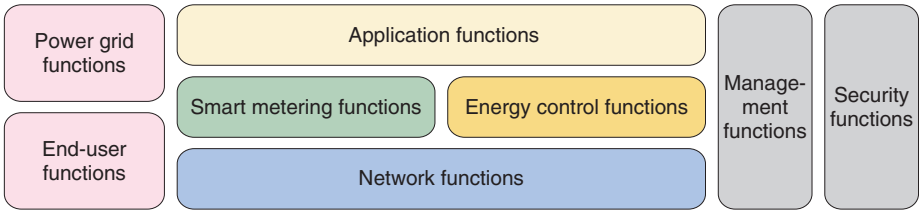


Fig. 3. Functional architecture model (under review).

ITU-T SGs and other SDOs, FG Smart will continue to edit and improve the deliverables and finalize them by the December 2011 meeting.

On the basis of FG Smart's output, a new study body for smart grids is scheduled to be approved in the January 2012 TSAG meeting. Since the technical area of smart grids is so wide-ranging, the candidates for this new body are expected to include a JCA (Joint Coordination Activity) or GSI (Global Standards Initiative), which are ITU-T study structures defined to span multiple SGs.

References

[1] FG Smart. http://www.itu.int/en/ITU-T/focusgroups/smart/Pages/Default.aspx
[2] N. Nagatsu, "Establishment of New Focus Groups in ITU-T", NTT Technical Review, Vol.8, No.8, 2010. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201008gls.html
[3] NIST's IKB. http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/IKBUseCases

Tsuyoshi Masuo
Senior Research Engineer, Supervisor, NTT Energy and Environment Laboratories.
He received the B.E. and M.E. degrees in systems engineering from Kobe University, Hyogo, in 1985 and 1987, respectively. He joined NTT Basic Research Laboratories in 1987 and studied software engineering and computer security. He moved to NTT Energy and Environment Laboratories in 2010. He is currently studying energy management systems and machine-to-machine communication.

NTT MSC
Expanding Offshore Outsourcing and Data Centre Business in the Third Most Attractive Business Location in the World

Fumitoshi Imaizumi†

President/CEO, NTT MSC Sdn Bhd

Abstract

Located in Malaysia—twice consecutively ranked as the third country, after India and China, as the leading outsourcing destinations in the world (Global Services Location Index (GSLI) 2011 by A. T. Kearney), NTT MSC has taken extensive steps to expand business operations in offshore outsourcing and data centre services. To provide confidence and reassurance to our customers and stakeholders, we secured ISO27001:2005 certification, the globally recognised international standard for information security, in April 2010 (ISO: International Organization for Standardization).

1. Introduction

1.1 Malaysia

Malaysia is strategically located in the heart of South East Asia, along the Straits of Malacca, one of the world's most important sea routes connecting Asia, Europe, and the Middle East. Separated by the South China Sea, Peninsular Malaysia is bordered by Thailand to the north and Singapore to the south while East Malaysia is situated on the island of Borneo, which Malaysia shares with Indonesia [1] (**Fig. 1**).

Located near the equator, Malaysia experiences a hot and humid tropical climate throughout the year with warm days and fairly cool nights. The rainy season varies with two monsoon seasons: the southwest monsoon from late May to September and the northeast one from October to February.

As of 17 June 2011, the Malaysian population was approximately 28.5 million, out of which Malays and other Bumiputera groups make up 65%, Chinese 26%, Indians 8%, and other unlisted ethnic groups 1%.

Fig. 1. Map of Malaysia.

† NTT MSC
No. 43000, Persiaran APEC, 63000 Cyberjaya, Selangor, Malaysia

Fig. 2. Sales office in the UBN Tower.

Multiculturalism has not only made Malaysia a gastronomical paradise, but also a country with colourful festivals.

Malaysia is a distinctive and peaceful country. The unity and vivid mesh between the complex diverse races, religions, and cultures is a unique characteristic of Malaysia. This multiethnic country, consisting of Malays, Chinese, Indians, Eurasians, and other races, has lived in a harmonised environment for generations.

1.2 NTT MSC Sdn Bhd

Established in 1997, NTT MSC Sdn Bhd, short for "sendirian berhad" (Malay equivalent to incorporated), was named after the renowned Multimedia Super Corridor (MSC), currently known as MSC Malaysia, a national information and communications technology (ICT) initiative conceptualised in 1996 as one of the main programs to accelerate Vision 2020—the strategic intent of the Malaysian government to transform Malaysia into a developed country by the year 2020.

NTT MSC's head office is strategically based in Cyberjaya, while the sales office is located in the heart of Kuala Lumpur's Golden Triangle (**Figs. 2** and **3**).

We were the first foreign company to be awarded MSC status, which is awarded to companies that develop or utilise internationally recognised multimedia technologies in their business activities. The status comes with a host of privileges including financial and non-financial incentives and world-class physical and communication infrastructure.

With years of experience in the Asia Pacific region, we are committed to providing the right solutions to corporate customers in order to meet their stringent individual business needs in ICT.

2. NTT MSC—our current services

As a wholly owned subsidiary of NTT Communications Corporation, NTT MSC provides enterprises, multinational companies, and service providers with one-stop business communication solutions. We offer ICT services such as NTT Communications' renowned Arcstar™*1 global private network services and Global IP Network services, data centre services, high-quality connectivity services, systems integration services, IT (information technology) management, and ICT-related services (IP: Internet

Fig. 3. Head office at Cyberjaya.

*1 Arcstar is a registered trademark of NTT Communications.

Photo 1. NTT MSC staff.

protocol).

Our Arcstar services are secure closed-network services that span more than 159 countries worldwide. Some of the key features of our end-to-end global connectivity solution include access to various connectivity technologies, customer support 24/7 from our multilingual helpdesk, monitoring and maintenance services, and service level agreements (SLAs) as part of our commitment to providing high service availability (**Photo 1**).

NTT Communications' Global Tier-1 IP Network service provides seamless Internet connectivity using a single autonomous system number. Through this world-class global tier-1 backbone, which covers Asia, Oceania, Europe, and North America, customers have direct connections to major Internet service providers in many countries, making Internet access faster with minimal delay. The high-quality Global IP Network service enables us to provide customers with the highest SLA in the Internet industry. This SLA applies automatically to customers of NTT Communications' IPv4 and IPv6 Transit Service and Collocation Connectivity Service.

Our data centre solution offers a full range of services to provide flexibility and scalability to cater for our customer's growing demand. Our data centres deliver a high-quality service based on innovative technology, a secure environment, and state-of-the-art facilities. We have built and designed our data centres to include reliable and redundant power and network infrastructure, effective cooling mechanism, and facility monitoring and management systems.

To complement our core services, we provide a full suite of fast and reliable Internet services, system integration services, and IT management services as a total one-stop ICT solution.

3. NTT MSC—our market potential

In spite of the moderate economic growth projection (5.2%) current year's and the fragility of the US recovery, there are still attractive opportunities in the ICT services area particularly as the Malaysian government implements measures to make Malaysia into a world-class data centre hub. The strong growth fundamentals and top initiatives that are expected to accelerate ICT growth are (1) ICT-friendly budget measures, (2) the National Broadband initiatives that push for greater broadband penetration, and (3) growing interest in cloud computing.

In terms of telecommunication services, fixed-line (wired) data communications is expected to grow 12.7% followed by wireless data and wireless voice at 10.3% and 3.8%, respectively. MPLS-enabled IPVPN service is expected to increase in line with the migration of ATM and frame relay services (MPLS: multiprotocol label switching, IPVPN: IP virtual private network, ATM: asynchronous transfer mode). PSTN (public switched telephone network) revenues will continue to decline as users shift to VoIP (voice over IP) technology.

4. NTT MSC—our strength

4.1 Global delivery and operations centre

In early 2011, we began full-scale operations of NTT Communications' Global Delivery and Operations Centre (GDOC). Through our collaboration and close relationship with Emerio, we are able to access an industry-relevant workforce and a greater pool of dedicated and experienced professionals. This multicultural multilingual team supports the Asia Pacific region, including China, Southeast Asia, and Japan, as well as other regions such as the USA and Europe.

At NTT MSC, GDOC supports the Arcstar Global Services by providing a full range of implementation, maintenance, monitoring, and management services. This is executed through three key functions: Arcstar Project Management, Arcstar Global Provisioning, and Arcstar Global Front. Their main activities are outlined below.

(a) These functions offer customers a complete set of network implementation services ranging from large-scale project implementation and

management and detailed network design to customer equipment configuration to meet the many stringent requirements of our customers.

(b) Together with teams in Tokyo, the USA, and Europe, the Global Provisioning Team carries out primary regional and global support work including processing order receipts, installations, and circuit operations to ensure that customers, network requirements are delivered with the highest quality and in a timely manner.

(c) The Global Front Team, which is available 24/7, works directly with our telecommunication partners, the NTT International Transmission and Maintenance Centre (ITMC), and the back-end Tokyo, New York, and London network operations centres (NOCs) to ensure that all customer requests and issues are resolved rapidly, appropriately, and within stipulated service levels, which are provided with all Arcstar services. The Global Front Team also works on all Level 2 or Level 3 node operation work, network monitoring, trouble isolation, and restoration.

(d) Regular monthly videoconference updates and key performance indicators monitoring between NTT Communications, the respective offshore centre function groups, and other stakeholders ensure the highest quality of services and functions for both the Global IP Network and Arcstar Global network services.

Having the GDOC team located within our 15.6-acre headquarters in Cyberjaya ensures that deployments and any expansion of global network services are undertaken swiftly and effortlessly. As the hub for the regional project managers and system engineers, NTT MSC is able to carry out large-scale project implementation and management, configuration, installation, testing, circuit operations, and support. GDOC works directly with NTT's telecommunication partners and regional NOCs to ensure that all customers' requests and issues are rapidly resolved within the stipulated service-level parameters, reinforcing our commitment to high-quality service.

4.2 Flexible and scalable data centre services

In Malaysia, we have two dedicated data centres located in Cyberjaya. They have been designed to cater for enterprises that require secure, resilient, and reliable data centre services as well as multinational companies that need quick, flexible solutions with high power requirements.

Data centre demand has continued to grow steadily over the past few years. Demand was further fuelled by the recent 9.0 magnitude earthquake in Japan, where requests for disaster recovery solutions—particularly disaster backup, recovery operations, and remote office sites—have increased. The increasing trend was consistent with our expansion plan to construct a third facility, which is expected to commence operations in the first quarter of 2012.

Fig. 4. New Cyberjaya 3 Data Centre.

Our new data centre, Cyberjaya 3 Data Centre (**Fig. 4**), which consists of a three-storey data centre and four-storey office building, comes with a modular design to address customers' needs for cost effective, energy-efficient, and scalable infrastructure solutions. This tier-3 data centre will offer customers a low total cost of ownership (TCO), equivalent to one third of the TCO in Japan. Equipped with a well-developed infrastructure and facilities that meet international standards, this data centre will emphasise green technology innovations including solar energy generation, rainwater harvesting systems, renewable energy technology, inverter techniques, and double-wall technology. Amongst the services offered at this data centre are disaster recovery solutions, cloud computing, and server consolidation platforms.

4.3 Multiservice telecommunication licences

After fourteen years of operations, we currently hold three out of the four different multiservice telecommunication licences in Malaysia. Achieving this as a wholly owned foreign company was possible only through our active participation in the development of the MSC and continuous commitment towards making Malaysia an ICT hub and regional centre for Internet traffic.

Since August 2000, we have held an Application Service Provider (Class) licence issued by the Malay-

sian Communications and Multimedia Commission (MCMC), the industry regulator in Malaysia. This licence enables us to provide specific services to end-users such as IP telephony services, Internet access services, and public switched data services.

In 2005, we were awarded the Network Service Provider (NSP) licence by MCMC for the provision of Global IP Network and Arcstar global private network services. The NSP licence authorises us to provide connectivity and bandwidth services that support a variety of applications. Subsequently, in Sept 2010, we received the Network Facility Provider (NFP) licence, which authorises us to offer network facilities services including fixed links and cables and a submarine cable landing centre.

Through such licences, we are working towards offering competitive products and services and introducing new Internet developments to further enhance the Internet industry in Malaysia.

5. Information security management

ICT has become a powerful enabler improving both communication and the exchange of information. As organisations become heavily reliant on ICT to support their core business operations, processes, and systems, they require assurance and peace of mind that their information is safeguarded.

To demonstrate our commitment to information security, we attained the ISO/IEC 27001:2005 certification in 2010 for our operations and supporting functions in Malaysia and for the delivery of services: specifically data centre and network services (IEC: International Electrotechnical Commission). The certification further validates that our operations and service provision have surpassed the rigorous requirements of the ISO standard.

The ISMS[*2] certification covers data centre and domestic network services and all critical business functions including network operations, data centres and IT managed centres, project management and implementation, sales, project strategy, corporate planning, accounting, purchasing, legal, human resources and administration, management information systems, product management, and business development.

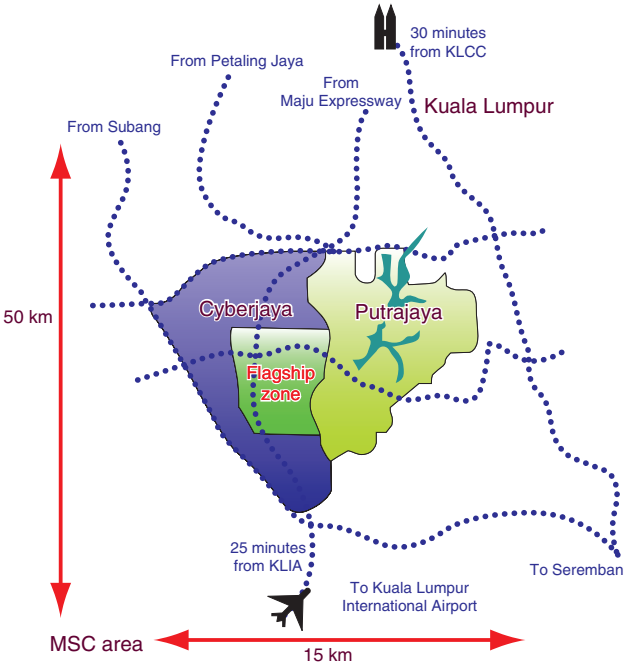


Fig. 5. Multimedia Super Corridor (MSC).

6. Social responsibility

In NTT MSC, we believe in contributing positively to our communities. To fulfil this commitment, we have participated in numerous projects that help create knowledge workers and build the ICT industry.

6.1 MSC Malaysia

Since 1996, NTT MSC and the NTT Group have contributed to the establishment of the MSC Malaysia Master Plan and the following flagship applications [2] (**Fig. 5**). They have actively participated in the MSC Malaysia project's initial planning stages and development. Specialist teams from NTT MSC and the NTT Group have worked on various aspects: the electronic government project with MAMPU (Malaysian Administrative Modernisation and Planning Unit), multipurpose smartcards with Bank Negara, the smart school project with the Ministry of Education, and telemedicine implementations with the Ministry of Health. All these projects were incorporated into the policy blueprint for MSC Malaysia flagship applications.

NTT MSC has seconded staff based at the Multimedia Development Corporation (MDeC) to advise on the construction of communications infrastructure and support Japanese investment in Malaysia, espe-

*2 ISMS is a part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.

Photo 2. NTT MSC head office official opening ceremony and MSF governor and scholars.

Photo 3. MSF governor and scholars.

Photo 4. MSF scholarship awarding ceremony.

cially in the MSC Malaysia area. For technology transfer, the NTT Group has worked together with MIMOS (Malaysian Institute of Microelectronic Systems) for the transfer of large-scale integration technology since 1998.

NTT MSC and the NTT Group have been recognised and commended by the Malaysian Government as active and strong supporters of the MSC Malaysia project. This commitment was demonstrated through the annual participation in the International Advisory Panel (IAP) by the NTT Group. The former President and CEO of NTT Communications Corporation, Masanobu Suzuki, personally attended most of the IAP meetings and continuously provided valuable advice and support to the Panel towards achieving the MSC Malaysia's objectives (**Photo 2**).

6.2 Multimedia Scholarship Foundation

Incorporated in March 1998, the Multimedia Scholarship Foundation (MSF) was a collaboration between NTT Corporation, NTT DATA, NTT Finance, and NTT Urban Development. Its objective was to provide financial assistance to undergraduates and postgraduates to pursue their studies at Multimedia University (MMU) Cyberjaya through a scholarship program (**Photo 3**).

This program is part of an initiative to support and develop knowledge workers as well as contribute to the growth of the ICT industry in Malaysia. As the program administrator, NTT MSC manages the scholarship fund, scholarship awarding process, and consequent employment opportunities with companies in the NTT Group. Since its inception in 1998, there have been more than 30 scholars in this program (**Photo 4**).

In addition to the scholarship program, we have contributed to MMU in other ways such as technical assistance, collaborative research and development activities, educational activities such as classes and seminars, research and development programs, advi-

sory activities, and planning for the university's educational enhancement program.

6.3 IT and HR seminars

We have endeavoured to contribute to IT and human resource (HR) development and knowledge transfer into Malaysia. One of the initiatives undertaken in early years of establishment was organising IT/HR-related complementary seminars to increase IT awareness among Malaysians.

NTT MSC together with the Overseas Vocational Training Association (OVTA) in cooperation with the Malaysian Ministry of Human Resources and the Japanese Ministry of Health, Labor and Welfare has organised Asia Pacific Economic Cooperation (APEC) IT/HR seminars in Malaysia. This yearly event is organised with the objectives of creating awareness of the benefits of IT and the influences of applying IT to business and management. Various distinguished speakers from industry and academia have been invited to share their knowledge, experience, and findings with the public.

References

[1] Department of Statistics Malaysia. http://www.statistics.gov.my/portal/
[2] Setia Haruman Sdn. Bhd. http://www.cyberjaya-msc.com/msc.asp

NTT MSC — short column

Open house

In Malaysia, festivities are commonly celebrated together by all communities and races through the *open house* tradition, where everyone is invited to join the festivities. This unique and distinctive tradition is practiced by all races in Malaysia.

NTT MSC Hari Raya Open House.

During the various cultural and religious festivals, friends, families, and even strangers are invited into the homes of those celebrating the festivals. All are welcomed with open arms and hearts to enjoy the special feast prepared by the hosts.

This tradition of celebrating cultural events together with those of the different races and cultures has helped create goodwill and improve tolerance and mutual understanding among communities and society. Even government officials participate in such activities by organising open house events at public halls where everyone is invited to enjoy the traditional delicacies and meet the ministers.

Wearing a jacket back to front

Motorcycles are a common sight on roadways throughout Malaysia. What is surprising to foreigners is to see a motorcyclist wearing his or her jacket back to front! It is not a local fashion trend but a means of protecting one's front from wind chill and arms from the strong sunlight. The hot humid tropical weather combined with wind chill makes it extremely unpleasant to wear a zipped- or buttoned-up jacket in the more usual manner. In fact, with the year-round heat, many Malaysians

Typical Malaysian motorcyclist.

tend to wear short-sleeved shirts or tops to keep cool. Thus, the simple jacket on the front serves two key roles for our motorcyclists: it protects the front upper torso from wind chill while allowing heat and moisture to escape from the back and it protect the arms from the scorching sun.

Lah!

When you speak to a Malaysian, you may notice the frequent usage of the word 'lah' in conversations, especially at the end of a sentence, regardless of the language. It may seem confusing at first, but this simple word can be applied in numerous ways to assert a position and entice solidarity. Commonly appended to the end of a word, it is often used to emphasise or reinforce a feeling such as 'Don't disturb me lah' or to soften a tone that may seem impolite 'No lah'. At times, it is used for reassurance, for example, 'Don't worry lah' or 'It's okay lah'.

Use of lah in daily conversation.

Lah is not a separate word by itself, so there is never a pause before it. And in spite of being common, it is not used at the end of every sentence. Using it properly is actually quite difficult for those who were not born into the language environment. It is a typical *manglish* word originating from the English, Malay, Hokkien, Mandarin, Cantonese, Tamil, etc., commonly spoken in Malaysia, reflecting the county's unique identity.

Malaysia batik

Malaysian batik is famous for its geometrical designs, leaves, and flower motifs. Unlike Javanese batik, Malaysian batik tends to have larger and simpler patterns with lighter and more vibrant colours. It is no surprise that with its historical significance and in line with the 1 Malaysia[*3] concept, the Malaysian government is now endorsing Malaysian batik as a national dress.

Batik designs.

This beautiful batik cloth was originally worn as casual and daily wear. Now, it is combined with modern fashion, and even a baby cradle has been commercialised. Batik has gained global and international recognition and is available in a variety of textile types for both men's and women's garments. Batik has been well received as one type of formal attire that can be worn to any formal event in Malaysia and it is commonly used for formal office wear.

With unlimited creativity in ideas nowadays, many other things have been created from batik including scarfs, neckties, furnishing fabrics, heavy canvas wall hangings, tablecloths, and household accessories. Although it is undeniable that batik is also produced in some other countries, Malaysia, with its own particular technique reflecting the unity of the country's multiculturalism and ethnic diversity, has given it a new touch and created a bigger presence in the current fashion industry.

*3 1Malaysia is an on-going programme created by the Prime Minister.

External Awards

Heisei 22 IPSJ Best Paper Award

Winners: Atsuhiko Maeda[*1], Hirohito Inagaki[*2], Minoru Kobayashi[*1], and Masanobu Abe[*3]

*1 NTT Cyber Solutions Laboratories
*2 NTT Cyber Space Laboratories
*3 Okayama University

Date: June 2, 2011

Organization: Information Processing Society of Japan

For "A Link Selection Technique Using "Arrow Tag" for Web Browsers on TV".

Television sets and video game consoles equipped with a web browser have appeared, and we are now able to browse web pages on television screens. However, existing navigation techniques are too difficult in this situation. In this paper, we propose Arrow Tag, a new link selection technique for web browsers on TV. In this technique, sequences of arrow signs called Arrow Tags are assigned to the links of the web pages, so a user can select the links by pushing the four direction keys a few times, while keeping her/his gaze fixed on the TV screen. User studies show that Arrow Tag significantly outperforms the conventional techniques of Focus Move and Number Tag. Moreover, most participants preferred Arrow Tag to either Focus Move or Number Tag.

Published as: A. Maeda, H. Inagaki, M. Kobayashi, and M. Abe, "A Link Selection Technique Using "Arrow Tag" for Web Browsers on TV," Transactions of the Information Processing Society of Japan, Vol. 51, No. 2, pp. 346–355, 2010 (in Japanese).

Best Paper Award

Winners: Lin Ma, Nobutomo Hanzawa, Kyozo Tsujikawa, and Shigeru Tomita, Advanced Media Research Group, Access Media Project, NTT Access Network Service Systems Laboratories

Date: July 6, 2011

Organization: The 16th Opto-Electronics and Communications Conference (OECC 2011)

For "Ultrawide-band WDM Transmission in a Multi-mode Fiber Using PCF Devices".

We demonstrate ultrawide-band (850 to 1550 nm) WDM transmission in multi-mode fiber by using single-mode photonic crystal fiber for center launching and as mode-filtering devices.

Published as: L. Ma, N. Hanzawa, K. Tsujikawa, and S. Tomita, "Ultrawide-band WDM Transmission in a Multi-mode Fiber Using PCF Devices," Proc. of OECC 2011, 6C2-3, Kaohsiung, Taiwan, July, 2011.