NICT NEWS

独立行政法人
情報通信研究機構

National Institute of Information and Communications Technology

2012 SEP
No. 420
9

01

World Record Cryptanalysis of a Next-Generation Cryptography

–Establishes security of pairing-based cryptography and contributes to its standardization as the next-generation cryptography–

Naoyuki Shinohara




03

Development of Navigation Technology for Assisting Visually Impaired People

–Enabling Real Time Positioning and Guidance With UWB Ranging and Smartphone–

Huan-Bang Li /Ryu Miura/Koji Yoshimoto/Kunio Tsutatani

05

Success in the World's First Automated Networking for Wide Area Network

–Easily Managed and Failure-Resistant. Substantial Progress Towards a Forthcoming New-Generation Network–

Kenji Fujikawa

World Record Cryptanalysis of a Next-Generation Cryptography

—Establishes security of pairing-based cryptography and contributes to its standardization as the next-generation cryptography—

Naoyuki Shinohara

Researcher, Security Fundamentals Laboratory, Network Security Research Institute

After completing a doctoral course, Shinohara joined NICT in 2009. He has engaged in research on security evaluation of public key cryptography. Ph. D. (Mathematics).

Background

Modern information systems dealing with confidential information such as for online shopping, Internet banking, and electronic applications to public institutions are increasing. For example, during a credit card transaction when internet shopping, the user enters and sends confidential information including a credit card number to a credit card company. In this case, encryption technology like public-key cryptography is used in order to protect the card's confidential information. Hence, it is indispensible to ensure the security of information by using encryption technology in order to allow users to transact information safely.

In recent years, many studies have been undertaken based on pairing-based cryptography[*1] including functional encryption and keyword searchable encryption as new cryptography suitable for clouds, which have the potential of applying many different services (Figure 1). For example, in a mail service using cloud storage, suppose a large amount of user's email is encrypted and retained on the cloud. Keyword searchable encryption can be used for keyword search on the encrypted emails. This allows users to search while search queries and emails stay encrypted without any decryption, enabling advanced privacy protection. Much attention has been paid to pairing-based cryptography as a next-generation cryptography because these cryptographic technologies suitable for clouds had not been achieved by traditional public-key cryptography[*2].

Pairing-based Cryptography Security and its Evaluation Method

While there are more reports on research achievements in pairing-based cryptography's fast implementation technology and applied technology such as keyword searchable encryption, its security was not sufficiently evaluated. And so, NICT conducted joint security evaluation research with Kyushu University and Fujitsu Laboratories Ltd. essential for putting pairing-based cryptography to practical use.

Now, I will briefly explain pairing-based cryptography's security and our method of evaluation (Figure 2). Pairing-based cryptography security is estimated by the computational cost to solve a discrete logarithm problem (DLP)[*3]. Factors in particular that relate to security are computing power, cryptanalysis's algorithms, cryptanalysis's time, and key size. Computing power indicates the computer's performance and is determined by the number of computers, cores, and core performance. Key size is the pairing-based cryptography's security parameter; as it becomes larger, the required time to break pairing-based cryptography increases. For example, in an environment with low computing performance where inefficient cryptanalysis's algorithm are utilized and cryptanalysis's time is short, cryptanalysis's capabilities are small and thus only small pairing-based cryptography keys can be cracked. On the other hand, if computing performance is high, cryptanalysis's algorithms are efficient, and

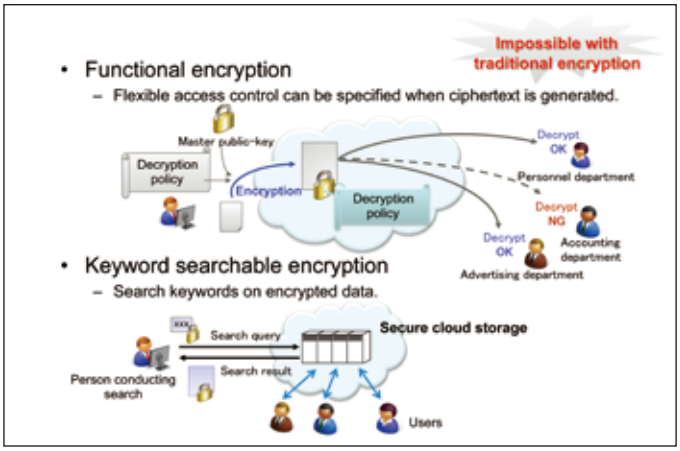


Figure 1●Prospect of pairing-based cryptography: cloud application

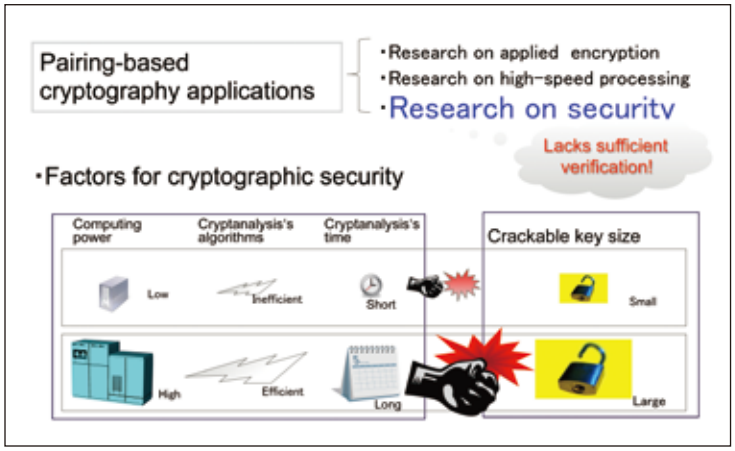


Figure 2●Pairing-based cryptography security evaluation(1)

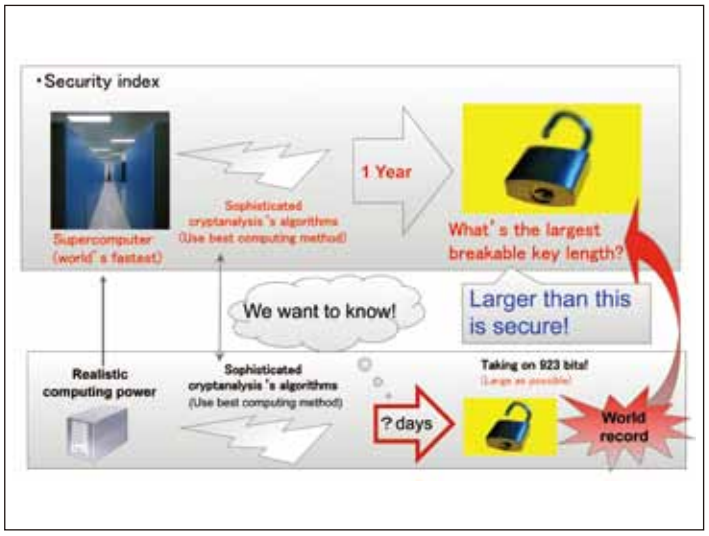


Figure 3●Pairing-based cryptography security evaluation(2)

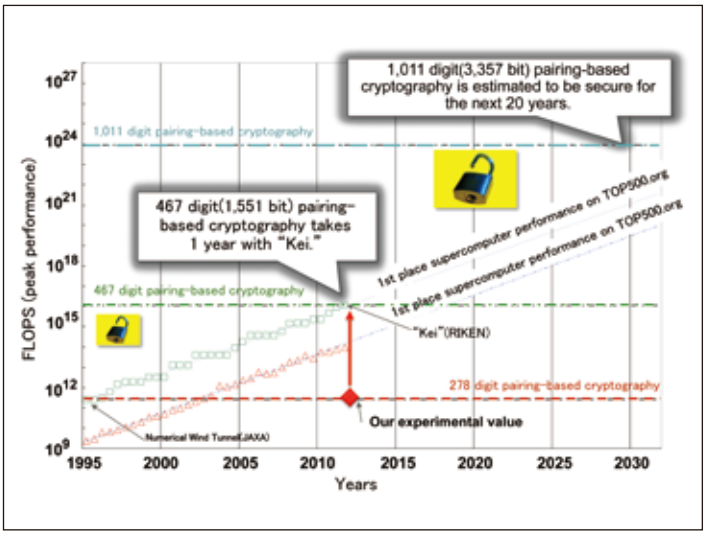


Figure 4●What's a secure key size in pairing-based cryptography?

enough cryptanalysis's time is allotted, even pairing-based cryptography with large keys can be broken. So, what is a secure key size? In general, a secure key size is considered one that cannot be cracked after a year of cryptanalysis's time using the world's fastest supercomputers and sophisticated cryptanalysis's algorithms (Figure 3). To estimate a secure key size, specifically, first you gather as many high-performance computers as possible, construct high-performance cryptanalysis's algorithms, and then run cryptanalysis's experiments on the largest key sizes possible, which is, in other words, an attempt to set a cryptanalysis's world record. By comparing the time it took to calculate by the computing environment used and that of the world's fastest supercomputer, you can identify the largest key size such that pairing-based cryptography can be broken at this time. Any keys with a size larger than that are considered secure keys.

Toward Secure Use of Pairing-based Cryptography, Challenging the World Cryptanalysis Record

To estimate a secure pairing-based cryptography key size, we attacked a 278 digit(923 bit)-long pairing-based cryptography that had been considered impossible to break without cryptanalysis for several hundred thousand years. And by creating new mathematical theories and fast implementation technology, we improved cryptanalysis's algorithms and succeeded with the cryptanalysis of that pairing-based cryptography by using 21 personal computers (252 cores) in 148.2 days. Based on the data attained from this world record breaking cryptanalysis experiment, we learned that, at this time, any key size larger than 467 digits is secure. Furthermore, given future computing performance growth projections, we find that 1,011 digit-long pairing-based cryptography will be secure for the next 20 years as shown in Figure 4.

Future Prospects

This result is not just a new world record of pairing-based cryptography cryptanalysis but also means the acquisition of valuable data that forms a technical foundation on which to estimate the appropriate timing to exchange a pairing-based cryptography key length. It also proves useful in the standardization of next-generation cryptography in electronic government systems in Japan and international standardization organizations.

Glossary

∗1 Pairing-based cryptography

A next-generation cryptography (proposed in 2001) based on a map called pairing, which offers many useful functionalities that could not be achieved by previous public-key cryptography. The security of pairing-based cryptography is based on the intractability of discrete logarithm problem (DLP).

∗2 Public-key cryptography

A cryptographic system requiring two separate keys, one to encrypt the plaintext, and one to decrypt the ciphertext. One of these keys is public and the other is kept private. Introduced by Diffie and Hellman in 1976. RSA and Elliptic curve cryptography (ECC) are typical examples.

∗3 Discrete logarithm problem (DLP)

A problem to compute integer d (logarithmic value) such that $a = g^d$ for given values g and a.

Development of Navigation Technology for Assisting Visually Impaired People

—Enabling Real Time Positioning and Guidance With UWB Ranging and Smartphone—

Huan-Bang Li

Senior Researcher, Dependable Wireless Laboratory, Wireless Network Research Institute

After completing a doctoral course, he joined Communications Research Laboratory, Ministry of Posts and Telecommunications (currently, NICT) in 1994. He is engaged in research and development in mobile satellite communications, UWB, and Body Area Network (BAN). He is currently a Visiting Professor at The University of Electro-Communications, Graduate School of Information Systems as well as the Vice Chair of IEEE802.15 Task Group 6. Ph.D. (Engineering).

Ryu Miura

Director, Dependable Wireless Laboratory, Wireless Network Research Institute

After completing a master's course, he joined Communications Research Laboratory, Ministry of Posts and Telecommunications (currently, NICT) in 1984. He is engaged in research and development in mobile satellite communications, stratospheric radio relay, inter-vehicle communications, Body Area Network (BAN), and disaster-resistant wireless networks. Midway, having transferred to and worked at Advanced Telecommunications Research Institute International (ATR) and other institutes, he became Director of Dependable Wireless Laboratory. Ph.D. (Engineering).

Koji Yoshimoto

Designer, Design Center, Marketing Unit, Fujitsu Limited

After completing a master's course, he joined Fujitsu Limited, Design Center in 2003. He is engaged in developing ICT universal design/barrier-free and ICT-based technology that assists persons with disabilities.

Kunio Tsutatani

Senior Expert, Design Center, Marketing Unit, Fujitsu Limited (Director of Universal Design)

After completing a master's course, he joined Fujitsu Limited in 1980. After working in the advertising department, he moved to the Design Center in 1999. Currently, he works as a Universal Design director with outside groups that promote Universal Design.

Background of Development

Today, various mobility assistance systems for visually impaired people are being developed. In recent years, GPS equipped mobile terminals are developed which identify the user's location and destination and provide voice guidance. However, an indoor mobility assistance system, where GPS cannot be used, has been a technological challenge and there is still no operated system in practical usage.

In collaboration between NICT and Fujitsu Ltd., we developed a mobility assistance system technology for visually impaired people by combining a high precision positioning UWB (Ultra Wide Band) system and a smartphone with mapping software and voice synthesis. The UWB positioning system identifies the user's present location, which is then displayed on smartphone via the mapping software and, in addition, voice guidance is performed to the indicated destination via smartphone operation. This system can even be utilized indoors where GPS cannot operate.

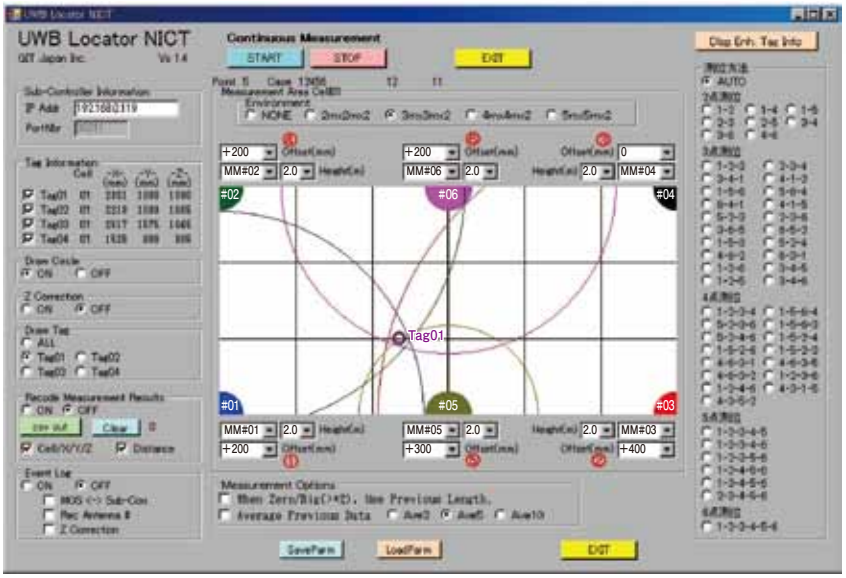


Figure 1●Screen display of Control PC's UWB positioning system

Positioning System that Utilizes IR-UWB

UWB, which spreads electrical power over an extremely broad range of radio frequency, is a wireless technology using low power density for communications as well as for ranging and positioning applications. Within UWB, the IR-UWB (Impulse Radio-UWB) is implemented by using extremely short pulses on the order of nanoseconds. Because a nanosecond pulse provides very precise time information, with Impulse Radio, measurement error will be less than 30cm. If distance is measured by 3 or more known base stations, the target mobile station can identify its own position. Figure 1 shows a screen display of the Control PC's positioning system using the developed IR-UWB.

With 4 in the corners and 2 in the center areas, total of 6 base stations (#01-#06) are arranged in the rectangular area in Figure 1. The mobile station (Tag01) that enters the area performs ranging with base stations capable of communicating and outputs each ranging results 5 times a second. Each ranging result is the average of over 20 measurements. These ranging results are then used by the Control PC to identify the mobile station position. Although positioning is possible if the distance from 3 base stations can be found, the positioning accuracy increases as the number of base stations increase. Base stations utilized in

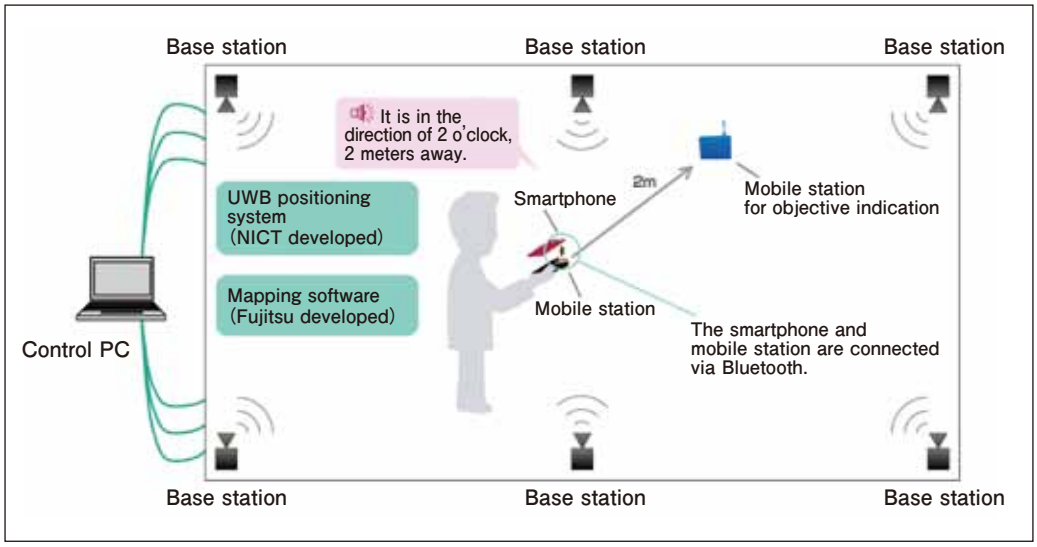


Figure 2●System usage image

positioning can also be designated. Moreover, Bluetooth is implemented in the user's mobile station which is used for data delivery with the smartphone.

System's Overall Structure and Prospective Usage

Figure 2 shows the system's overall structure and usage example. It is composed of 6 base stations arranged as infrastructure, the user's mobile station as well as the mobile station for objective indication, and the PC that controls the entire system. First, based on ranging results, the Control PC identifies each two-dimensional coordinate value that shows the positions of the user's mobile station and mobile station for objective indication. Next, the two-dimensional coordinate results are sent in real-time to the user's mobile station and also forwarded via Bluetooth to the smartphone. The smartphone uses the two-dimensional coordinates to display the user's position and the destination's position on the smartphone's mapping software. In addition, the walking direction and distance to arriving at the destination is announced with voice synthesis. The two-dimensional coordinates, mapping software's position display as well as the voice guidance content are updated as the user moves.

Although in this project we arranged a mobile station to the destination, this is not necessary if the mapping software is revised to allow the destination data to be set. Mobile stations can be utilized on any object with an unfixed position.

Smartphone Mapping Software and Voice Synthesis

The mapping software was developed for Android 2.3. You can import the images such as the map of the exhibition, or you can add introduction video of the exhibition (Figure 3). When you activate the mapping software, your current location is displayed on a map. Once you select the place you wish to go with the "Navigate" button, the direction and distance to that location is read aloud. Using Android's standard application interface, the audio reading is made to read aloud with the voice synthesis pre-installed library.

Figure 3●Objective settings screen

By pressing the "Read" button while moving, you can reconfirm the direction and distance to the destination at anytime. The directions from front-to-back, left-to-right, on an angle, and ones in between can be shown as numbers of a clock ("2 o'clock direction," etc.). In addition to audio reading, an animation of your current position and the destination location is displayed on the screen for sighted users (Figure 4). When you arrive to the destination, a sound and vibration occurs, and the configured video is played automatically.

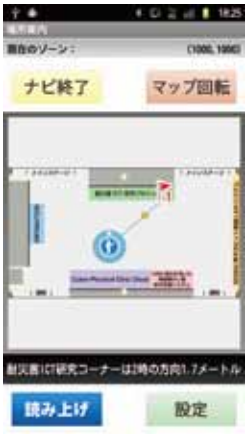


Figure 4●Mapping software navigation display

Conclusion

In this project, we successfully developed a system that notifies the distance and direction to a target destination in one's surroundings by combining a UWB positioning system and smartphone mapping software and, once arriving at the target destination, automatically notifies the user with a voice description of the destination.

When providing voice guidance to visually impaired people, information on obstacles along the path is important. Hereafter, we will further our technological development in the field of assistance for visually impaired people by constructing a system that combines the detection of obstacles along a path.

In addition, we expect that this high precision ranging technology is not limited to visually impaired people but also applied to indoor guidance services for general users. For example, by providing contents adapted to a place such as large corporate/government buildings and hospitals for safety/security improvement with guidance, museums, galleries, libraries, and shopping malls, we believe this can be applied to integrated support services that lead to fun and comfort.

Success in the World's First Automated Networking for Wide Area Network

—Easily Managed and Failure-Resistant. Substantial Progress Towards a Forthcoming New-Generation Network—

Kenji Fujikawa

Senior Researcher, Network Architecture Laboratory, Photonic Network Research Institute

After completing a graduate course, Fujikawa served as a Kyoto University Graduate School assistant professor from 1997 and as a senior researcher at ROOT Inc. from 2006 and joined NICT in 2008. He is engaged in new-generation network architecture research.

Background

In order to secure alternate routes in the current Internet, organizations such as businesses and data centers acquire an independent address space (aggregation of location information) and connect with multiple upper ISPs(Internet service providers). Afterwards, communication becomes possible when routing information including address space within the organization is advertised to an outside upper ISP. Today, routing information advertises amounts up to 400,000, which makes it time-consuming to detect non-functioning routing information and therefore hinders rapid switching to alternate routes when a network failure occurs (Figure 1).

In order to quickly secure alternate routes, it is effective to receive allocations from multiple address spaces by multiple uppers than organizations using specific address space (details below). However, this increases address information that can be manually configured, which makes the task more complicated and therefore causes human errors in operational management. Hence, this method is currently unpopular.

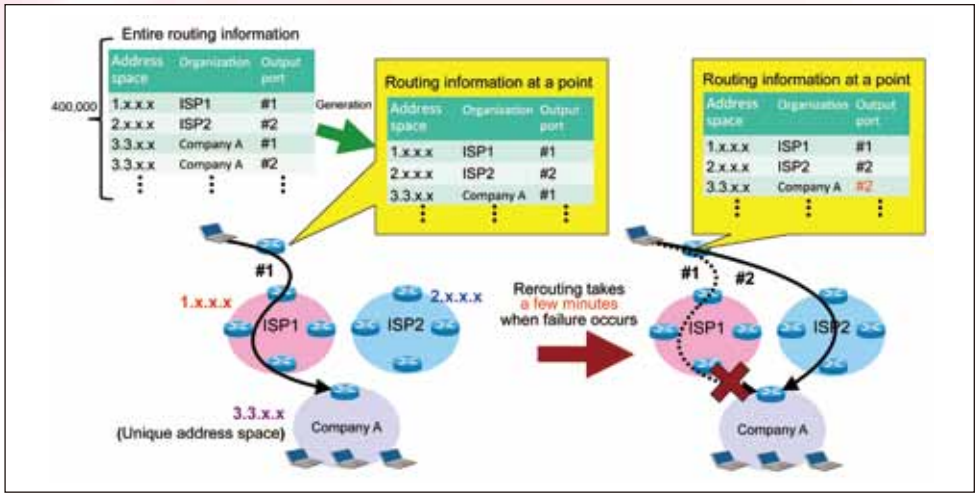


Figure 1●Route switching during wide area network failure

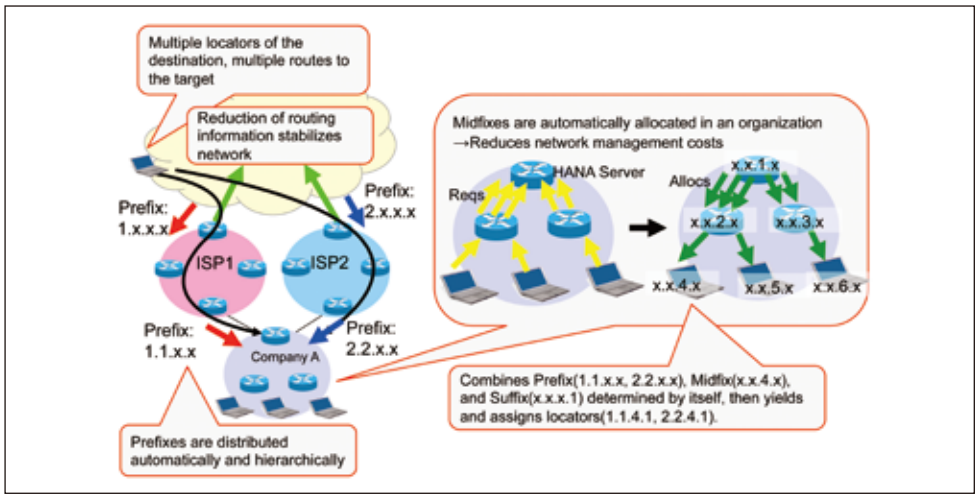


Figure 2●Overview of HANA

HANA Design and Implementation

At the Network Architecture Laboratory of the Photonic Network Research Institute, we are advancing research and development of highly-available networks that improve reliability by preparing against network communication failures caused by overload and equipment failure due to concentrations of communication data, by simplifying and automating multihome network architecture and management that establish multiple communication routes, and by supporting heterogeneous communications.

As part of this effort, we redefined an address, which is location information within the Internet, as a locator, and designed and implemented the HANA (Hierarchical and Automatic Number Allocation for locators) protocol, which hierarchically and automatically allocates and assigns locators (Figure 2). Thus

far, automatic allocation of addresses could only be performed in terminals such as PCs, but in HANA, locators are automatically allocated to routers and servers in addition to terminals. HANA supports IPv4 as well as IPv6 address systems and can even support new address systems defined in the future (however, in Figure 2, only IPv4 addresses are indicated).

In HANA, locator prefixes are distributed hierarchically, and if an organization is connected with multiple upper ISPs, multiple prefixes are allocated. The middle part of a locator, the midfix, is uniquely allocated within a domain independent of prefix allocations. PCs, routers, and servers determine the lower part of the locator, the suffix, and yields locators by integrating allocated prefixes and midfixes. If multiple prefixes are allocated, multiple locators are generated.

When an organization, without securing independent locator space, is allocated a part of a locator space as a prefix from a connected ISP, specific route information of the domain is not advertised to outside routers and Internet route information is reduced (Figure 3). Moreover, when the organization connects to multiple ISPs, it can use different routes via designated destination locators. When a failure occurs, an alternate route can be selected by just switching the destination locator that will be used. Thus a quick way to route switching is provided. While it is necessary to allocate multiple locators within organizations, HANA does not increase operational management costs thanks to its automatic configuration.

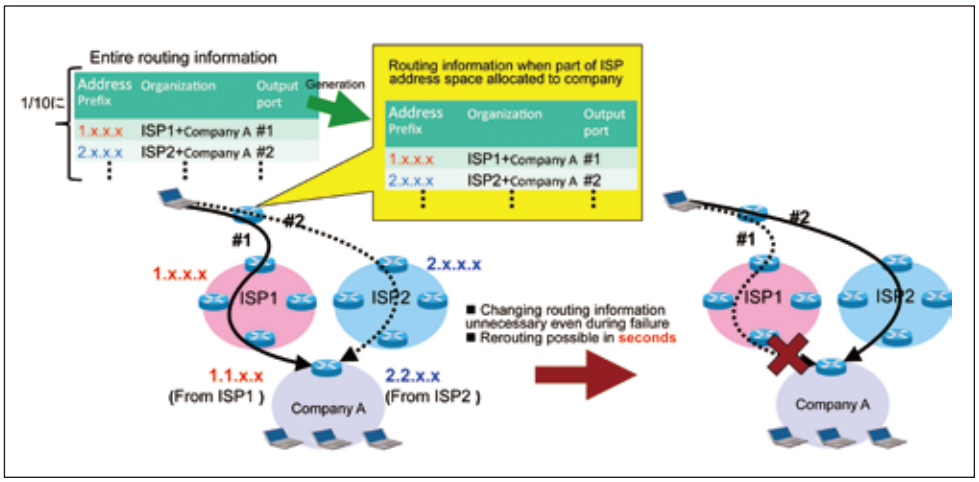


Figure 3●Route switching when using multiple locators

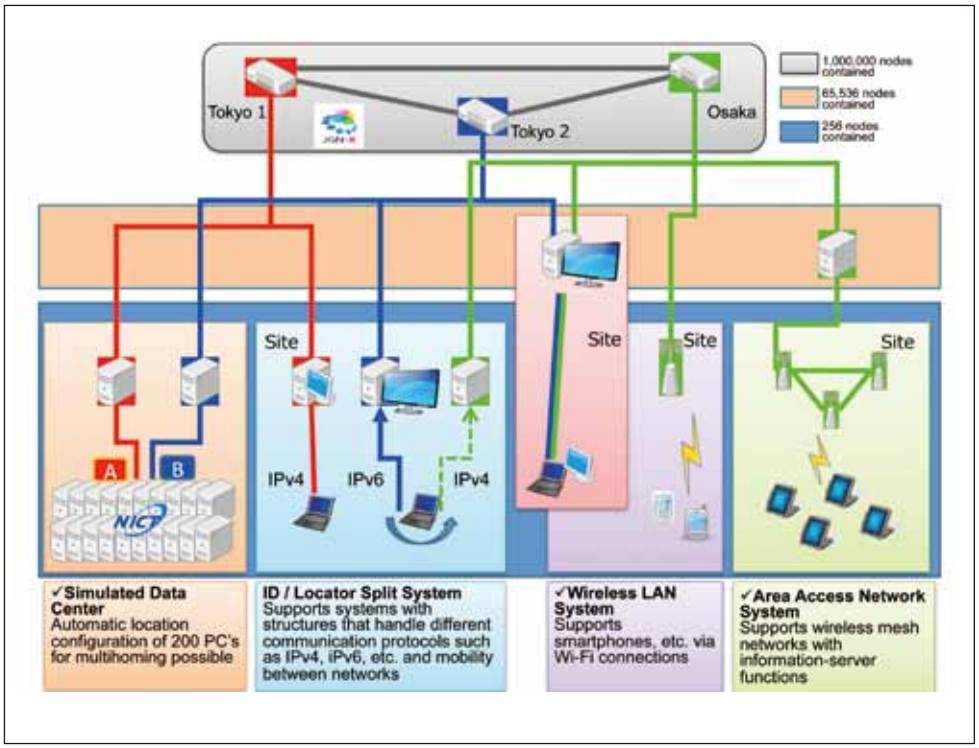


Figure 4●Wide area network automatically constructed using HANA

Construction of a Wide-Area Network with HANA

In this project, we automatically configured a wide-area network with HANA on JGN-X, a new-generation communication network testbed (Figure 4). The automatically constructed wide-area network consists of an emulated data center in the laboratory and networks based on IPv4/IPv6 user terminals. Besides PCs, multiple locators are also automatically allocated for routers and servers that have been manually configured up to now. With each device holding multiple locators, efficient rerouting is ensured when failure occurs.

By using our results in the management of a wide-area network, we bring automation and higher efficiency in operational management tasks. Also, rerouting assurance was simplified and a failure-resistant, highly-available network is successfully constructed.

A demonstration exhibit was held June 13~15, 2012 at Makuhari Messe during Interop Tokyo 2012.

Future Prospects

For future work, we will increase HANA-constructed network hubs and demonstrate that it can be applied to wider area networks as well as large-scale data centers. In addition, in our laboratory, we plan on advancing Integration of HANA and HIMALIS(Heterogeneity Inclusion and Mobility Adaption through Locator ID Separation) and establishing a route selection method that actively utilizes multiple locators.

Prize Winners

Prize Winner ● **Masahide Sasaki** / Director, Quantum ICT Laboratory, Advanced ICT Research Institute
Mikio Fujiwara / Senior Researcher, Quantum ICT Laboratory, Advanced ICT Research Institute

◎Date: 2012/3/16

◎Name of Prize:

Maejima Award

◎Details of Prize:

For their contribution to pioneering work on quantum ICT and realization of secure movie data transmission using quantum key distribution.

◎Name of Awarding Organization:

Teishin Association

◎Comments by the Winner:

We are very grateful to receive such a prestigious award. We received this award on behalf of all the people inside and outside our institute who were involved in our research and development now and in the past. We were able to engage in dynamic research and development in an unprecedentedly privileged environment with wonderful colleagues under the leadership of the Ministry of Internal Affairs and Communications, through encouragement and guidance from successive executives and superiors.

Masahide Sasaki

Mikio Fujiwara

Prize Winner ● **Shigehito Miki** / Senior Researcher, Nano ICT Laboratory, Advanced ICT Research Institute

◎Date: 2012/4/17

◎Name of Prize:

The Young Scientists' Prize of the Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology

◎Details of Prize:

In recognition of distinguished research achievements that demonstrate advanced research and development ability in a scientific field of Japan, communication wavelength superconductivity nano-wire single-photon detector research.

◎Presenter of Award:

Minister of Education, Culture, Sports, Science and Technology

◎Comments by the Winner:

I received this award due to highly acclaimed research and development of communication wavelength high-performance single-photon detectors that utilize superconductive nano-wire. I would like to express my appreciation to family and everyone who has cooperated and guided me as I progress with this research. I will continue doing my best to achieve even better results.

Summer Science Camp 2012 Report

Summer Science Camp 2012* was held at the Universal Communication Research Institute (Keihanna) for three days from July 25 – 27, 2012. This year, under the theme of "Let's unravel it! Reality Feeling System with Pictures and Sounds," 10 high school students selected out of many applicants participated.

During the three-day camp, members of Multisensory Cognition and Computation Laboratory held lectures (Stereoscopic systems and 3D display, Systems of 3D audio), practical training (Construction and analysis of 3D audio, fMRI measurement and data analysis on brain activity for visual sense), and a facility tour and hands-on demonstration.

On the last day, student apprentices held themed presentations, and at the closing ceremony, each student was handed a completion certificate from Dr. Hiroshi Ando, Director of the Multisensory Cognition and Computation Laboratory.

Feedback from participants included the following comments; "It was really helpful in deciding the university department to apply for in the future," "I learned the importance of physics and mathematics through this course," and "I learned that various kind of knowledge is necessary for even one research, and I will actively devote myself to all my studies from now on."

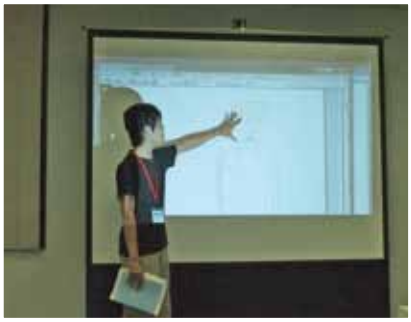
* Science/technology training camp program under the sponsorship of Japan Science and Technology Agency and run/operated by Japan Science Foundation at host universities and public research institutes that aims to enhance exchanges among researchers, engineers, and participants through lectures and training that utilize the characteristics of host institutions for high school and technical school students.

●Remarks from Director General, Dr. Yutaka Kidawara

●Experiencing Multichannel Speaker-Array System

●Training and lecture on 3D audio system

●Analyzing the data measured with fMRI



●Themed presentations by student apprentices

●Receiving a completion certificate at the closing ceremony

Advanced ICT Research Institute Report on Facility Open House

– Experience the future of information and communications!! –

The Advanced ICT Research Institute (Kobe) held an open house event for the public on Sat, July 28, 2012. With great weather, a total of 597 visitors attended. Many visitors participated in the popular annual quiz rally where they toured each research group booth in the order of the quiz and enjoyed the elaborate interactive exhibits and interacting with the researchers. There was also exhibit from the Applied Electromagnetic Research Institute's Space-Time Standards Laboratory.

Display exhibition

●Introduced the latest research that utilizes quantum mechanical properties such as quantum cryptography, quantum communication, quantum clocks, etc.
(Quantum ICT Laboratory)

●Experienced the cryogenic phenomena at below cryogenic temperature (-120°C) due to superconductivity phenomenon.
(Superconductive Device Group)

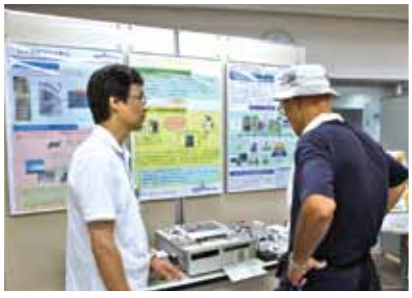
●What do things look like through a transparent terahertz wave?
(Terahertz and Millimeter wave ICT Laboratory, Terahertz Research Center)

●Experienced birefringence and polarization by making 3D glasses and polarization boxes using polarization sheets.
(Organic Nano-Device Research Group)

●Extracted broccoli DNA, touched it, observed it under a microscope.
(Bioinformatics Group)

●Made a Leeuwenhok microscope and observed the micro-world under original microscope.
(Biophysical Group)

●Experienced the relationship between emotions and brain decisions through a simple game.
(Brain Information Group, Center for Neural Systems and Information Networks)



●Detailed explanation on how Japan Standard Time is made and distributed.
(Space-Time Standards Laboratory)

●Safeguarded radio waves. Introduced radio wave surveillance systems.
(Kinki Bureau of Telecommunications)

In the fifth research lecture meeting, many talks were given using familiar examples to introduce the fields of nano, bio technology and to explain the latest research reports. The room was full for both morning and afternoon lecture meetings with participants from a broad range of ages listening intently. In Q&A sessions after each lecture, participants threw many sharp questions in a comfortable atmosphere and enjoyed the lectures and direct conversations with the researchers.

●Lecture meeting room

Lecture meeting scene

"Clarify the Homologous Chromosomal Pairing Mechanism"

Daqiao Ding
Senior Researcher, Bio ICT Laboratory

"Handling Matter in the Nano-Meter World"

Shukichi Tanaka
Research Manager, Nano ICT Laboratory

"Observe the Dreaming Brain"

Satoru Miyauchi
Chief Senior Researcher

Children's Day for Visiting Kasumigaseki Report

– Experience Earth Seen from Space with a Digital 4-Dimensional Globe! –

On August 8–9, 2012, NICT participated in Children's Day for Visiting Kasumigaseki under the auspices of the Ministry of Internal Affairs and Communications. This event is initiated by the Ministry of Education, Culture, Sports, Science and Technology in collaboration with ministries and agencies in Kasumigaseki, in order to give children an opportunity to see and learn about society through work explanations and government ministry tours during summer vacation, and to promote policies of ministries and agencies.

This year, NICT featured an exhibit using a 4-dimensional digital globe, "Dagik Earth." Dagik Earth uses a projector to project images on a spherical screen to display a globe. In this exhibit, many things were displayed such as concentrated waves in the ionosphere propagated by the 2011 off the Pacific coast of Tohoku Earthquake, environments of the globe, and celestial objects from places such as the moon.

Our exhibit was so impressive and got much attention from the participants.

●Children experiencing the NICT booth

Exhibit Collaborator: Graduate School of Science, Kyoto University
The Earth Science Hub Dagik Team

Dagik Earth was supported by a grant from the Ministry of Education, Culture, Sports, Science and Technology (MEXT) of Japan between FY 2009–2011 to develop the system and educational programs. Kyoto University, NICT, National Museum of Nature and Science, Shizuoka Science Museum, and Shizuoka University participated in this project.

Keihanna Information and Communication Fair 2012

—Leading the Future of Science and Technology with Information and Communication—

free admission

In partnership with "Keihanna" Kansai Science City's information and communication-related institutes, NICT Universal Communication Research Institute will hold a community-based collaborative event, "Keihanna Information and Communication Fair 2012," on November 8th(Thu) ~ 10th(Sat), 2012. This event aims to spread news on research achievements in information and communication technology and promote mutual collaborations between related institutes. Please join us.

Main Exhibits

●World's largest 200-inch multi-view glasses-free 3D images

●Network-based voice translation application "VoiceTra4U-M"

Main Talks

"Front-Line Cyber Security Techniques"
Daisuke Inoue
Director, Cybersecurity Laboratory,
NICT Network Security Research Institute

"Information Analysis Technology for Tackling Increasingly Complex Social Phenomena"
Kentaro Torisawa
Director, Information Analysis Laboratory,
NICT Universal Communication Research Institute

"Source of Japan Standard Time
~Gathering Science and Technology for the Ultimate Standard~"
Mizuhiko Hosokawa
Executive Director,
NICT Strategic Planning Department

There will also be many more exhibits and talks on leading-edge research results.

Venues: Keihanna Plaza, ATR, SCSK, Kansai-kan of National Diet Library
Date: November 8th(Thu)~10th(Sat), 2012
※Registration Webpage for participants on the 8th (online registration accepted)
http://khn-fair.nict.go.jp/

Facility Open House 2012

free admission

● Kashima Space Technology Center

Venue: Kashima Space Technology Center
893-1, Hirai, Kashima, Ibaraki 314-8501
http://ksrc.nict.go.jp/
Contact: 0299-82-1211
Date: November 23, 2012 (Fri / Holiday) 10:00~16:30(reception until 16:00)

● Okinawa Electromagnetic Technology Center — 10th Annual Facility Opening with Many Fun Events!! —

Venue: Okinawa Electromagnetic Technology Center
4484, Aza-Onna, Onna, Kunigami, Okinawa 904-0411
http://okinawa.nict.go.jp/
Contact: 098-982-3705
Date: November 23, 2012 (Fri / Holiday) 10:00~16:30(reception until 16:00)

Information for Readers

The next issue will feature topics including three element technologies for new-generation ICT services and a echnology for flexible privacy protection on networks.

NICT NEWS No.420, SEP 2012
ISSN 2187-4034 (Print)
ISSN 2187-4050 (Online)

Published by
Public Relations Department,
National Institute of Information and Communications Technology
<NICT NEWS URL> http://www.nict.go.jp/data/nict-news/

Editorial Cooperation: FULFILL co., ltd.

4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
Tel: +81-42-327-5392 Fax: +81-42-327-7587
E-mail: publicity@nict.go.jp
<NICT URL> http://www.nict.go.jp/