独立行政法人
情報通信研究機構
NICT NEWS
National Institute of Information and Communications Technology

MAR. 2013
No. 426
3

Security Evaluation of Cryptographic Technology

MORIAI Shiho

Director of Security Fundamentals Laboratory, Network Security Research Institute

Graduated in 1993. Joined NICT in 2012 after working at Nippon Telegraph and Telephone Corporation and Sony Corporation. She has been engaged in research on design and analysis of cryptographic algorithms and international standardization of cryptographic technology. Ph.D. (Engineering).

Importance of security evaluation of cryptographic technology

With advancements in networks, cryptographic technology has become a fundamental technology that sustains the foundations of modern society. The use of cryptographic technology is not just in preserving security of communications on the Internet and mobile phones but also in automatic ticket gate systems for railway passengers, electronic toll collection systems on the highway, content distribution of e-books etc., copyright protection on Blu-ray disks, and IC chip-embedded passports to prevent forgery. It is fair to say that safe and secure communications, business, and transportation are now unthinkable without cryptographic technology.

However, cryptographic technology commonly used in today's society does not maintain permanent security; even once security is confirmed, advancements in cryptanalysis may bring about rapid security deterioration. Therefore, at the Security Fundamentals Laboratory of NICT Network Security Research Institute, we are conducting continuous research on security evaluation of cryptographic technology taking into consideration the improvement of ever-advancing cryptanalysis/computing capabilities.

Security strength

How can we evaluate security of cryptographic algorithms? The security of a cryptographic algorithm is defined as a number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm with the most efficient algorithm. If the attack complexity was the order of 2^k, we say that the cryptographic algorithm's security is k bits. For example, if the key of Algorithm A is recovered with 2^{112} times of decryption operations, Algorithm A provides 112 bits of security (Figure 1). When evaluating cryptographic security, one should find the most efficient attack algorithm and, with that method, it is estimated how much work should be necessary for the attack.

Taking into account the improvement of computing capabilities and cryptanalysis advancements, the US National Institute of Standards and Technology (NIST) releases recommendations on what level of security and for how many years certain cryptographic technologies should be used for US government procurement. Figure 2 shows the recommended key lengths and parameters that NIST announced in 2007. This shows that one should use cryptographic technology with at least 112-bit security from 2011 and that symmetric key cryptography equivalent to this level is 112-bit key length, public key cryptography based on integer factorization problem such as RSA is 2048-bit key length,

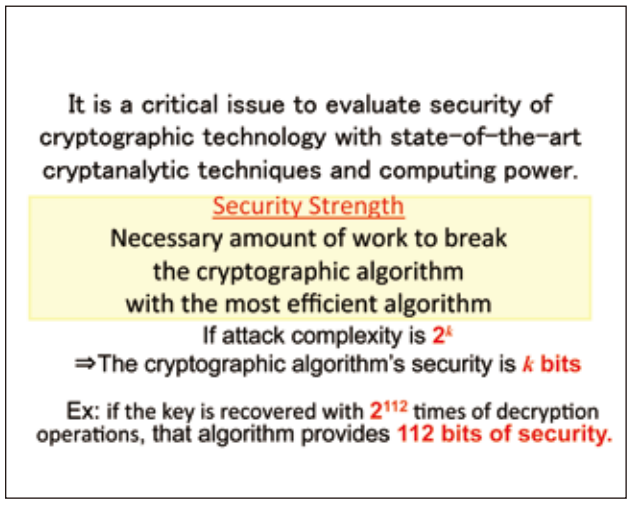


Figure 1 Security evaluation of cryptographic algorithms

		Key Lengths / Parameters (bit)				
		~2010	2011~2030	2031~	2031~	2031~
Security Strength		80 bit	112 bit	128 bit	192 bit	256 bit
Symmetric Key Cryptography (AES, etc.)		80	112	128	192	256
Public Key Cryptography	Algorithms based on Integer Factorization Problem (RSA, etc.)	1024	2048	3072	7680	15360
	Algorithms based on Discrete Logarithm Problem (DSA, DH, etc.)	1024	2048	3072	7680	15360
	Algorithms based on Discrete Logarithm Problem on Elliptic Curves (ECDSA, ECDH, etc.)	160	224	256	384	512
Hash Functions (SHA-2, etc.)		160	224	256	384	512

Recommendation for Key Management – Part 1: General (Revised), NIST SP 800-57, 2007.

Figure 2 Security strength

public key cryptography based on discrete logarithm problem such as DSA is 2048-bit key length, public key cryptography based on discrete logarithm problem on elliptic curves such as ECDSA is 224-bit key length, and hash function is 224-bit hash length. Note that this index was shown by NIST in 2007 based on an asymptotic complexity evaluation and will continue to change based on evaluation results from ever-advancing technology and actual computer experiments. Besides NIST, research institutes in other countries are also releasing recommendations, some of which show recommended key lengths and parameters different from NIST.

Achievements in the Security Fundamentals Laboratory

Cryptographic security evaluation performed at the Security Fundamentals Laboratory includes evaluations on elliptic curve cryptography and RSA — currently the most widely used public key cryptography. In particular, breaking 1024-bit RSA has been found to be much easier than previously assumed; today, it has been evaluated that it takes approximately one year for supercomputer "Kei" to solve (Figure 3). This evaluation result has been made public through CRYPTREC (Cryptography Research and Evaluation Committees) — a project that observes and evaluates the security of e-government recommended cryptography of Japan and investigates and reviews appropriate implementation and operating methods for cryptographic technology. At our laboratory, we are making contributions to CRYPTREC secretariat and cryptographic security evaluations for revising the e-Government Recommended Ciphers List. Details are introduced on page 6 of this issue.

We are not only performing security evaluations on currently-used cryptographic technology but also, next-generation cryptography for cloud computing that will allow data processing on encrypted data in order to be able to outsource computing tasks without revealing any content to others. With this evaluation, we can determine what parameters to select to ensure security in next-generation cryptography, which leads to practical use of next-generation cryptography and standardization. Regarding security evaluation of next-generation cryptography, our laboratory has so far achieved a world record for the decryption of "pairing-based cryptography" that realizes an advanced privacy protection function (published in NICT NEWS September 2012 issue). We also achieved a world record on security evaluation of lattice-based cryptography. Details are introduced on pages 3-5 of this issue.

Security evaluation results on cryptographic algorithms conducted by NICT are making vital contributions by providing a technological basis for the e-Government system of Japan and for selecting suitable key lengths and parameters to securely use cryptographic technology that is widely used throughout the world.

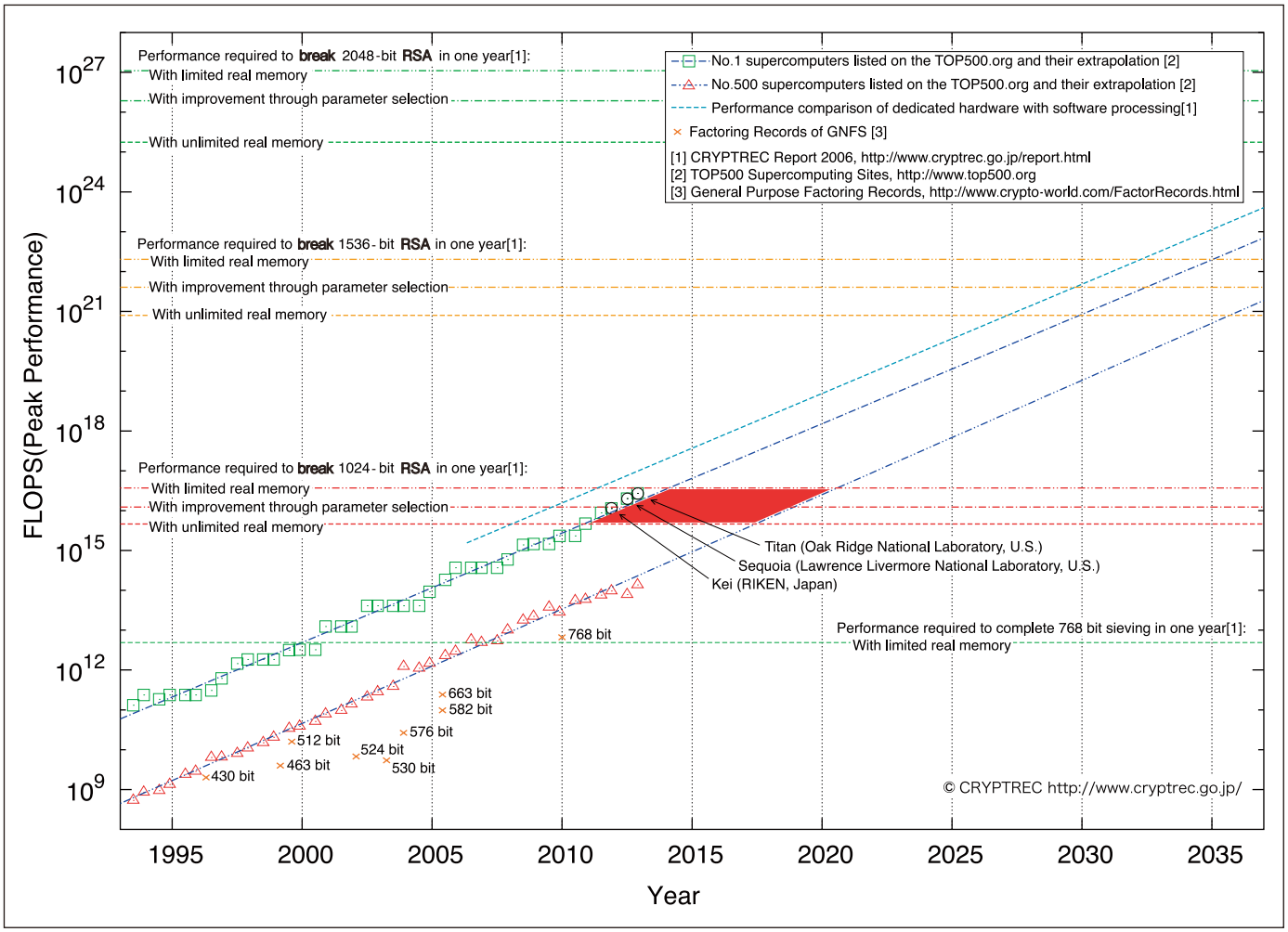


Figure 3 Security evaluation of RSA

The vertical axis shows computing performance and the horizontal broken lines in the graph show the performance required to break RSA in one year, from bottom to top, of 768-bit, 1024-bit, 1536-bit, and 2048-bit. Note that this performance varies depending on whether there are real memory limitations—for example, 1024-bit RSA is shown with several red broken lines. The lines extending from the bottom left to the top right of the graph show the improvement in shifting computing performance year to year, and the performance of supercomputers ranked 1st (□) and 500th (△) place in the TOP500 list, which presented a ranking from 1–500 of supercomputer computation speed, are shown via the extrapolation lines. The points where the horizontal and diagonal lines intersect, painted in red, show the period it takes to break 1024-bit RSA in a year using a supercomputer. As of 2013, we have reached the point where 1024-bit RSA can be broken in one year using a supercomputer.

Security Estimation of Lattice-Based Cryptography

—The first step to practical use—

AONO Yoshinori

Researcher, Security Fundamentals Laboratory, Network Security Research Institute

After completing a doctoral course, joined NICT in 2011. He has been engaged in security analysis of public key encryption schemes. Ph.D.(Science).

Introduction

To keep the security of our social activities, several cryptographic technologies are used in communication infrastructures and digital equipments; particularly, the RSA cryptography and the elliptic curve cryptography are widely used. However, about 20 years ago, it was proven that these two cryptographies are easily broken by using a quantum computer. After this, researchers have tried to invent cryptographic schemes resisting both quantum and normal computers, which are usually called post-quantum cryptography.

Several candidates of such cryptographic schemes are now proposed, and efforts are being made to implement them. Researchers found that some of the candidates are not only secure but have various useful properties. For example, they can be used for protecting data in cloud computing and managing information in a large organization, which were hard to realize when using RSA or elliptic cryptography. Proposers of these candidates are claiming the schemes' advantages and suitability of being the de facto standard of post-quantum cryptography. Now, it must be decided which candidate is best to implement in society.

Which is the best cryptography?

—Computer experiments for estimating the practical strength—

In order to decide which scheme is best, it needs to compare candidates in a uniform standard. For example, consider a cryptographic scheme of short key length and that of long key length. It is clear that the latter one is more secure. However, this idea is not valid when comparing two different schemes. To solve this problem, researchers in cryptographic areas have decided to use computational time for breaking cryptographic schemes of a certain parameter. For example, this is done for each candidate, by estimating the smallest parameter that takes over one year to break the scheme by Supercomputer Kei using the fastest program in the world, and then comparing the encryption speeds for the parameters.

In fact, because both supercomputers and algorithms for analyzing cryptographic schemes continue to improve, we need to predict the performance of the latest supercomputer in the future and lowest parameters that require a year by such supercomputers. The results are drawn in the graph as Figure 2 and 3. Of course, since we cannot use the supercomputer throughout one year in actuality, we perform a computer experiment of smaller scale and extrapolate the results. In order to know which candidates are better for post-quantum cryptographies, researchers have improved the algorithms and carried out such preliminary experiments. Recently at the Security Fundamentals Laboratory, we estimated the practical hardness of *the shortest vector problem* in which the security of lattice-based cryptography is based, one of the post-quantum candidates.

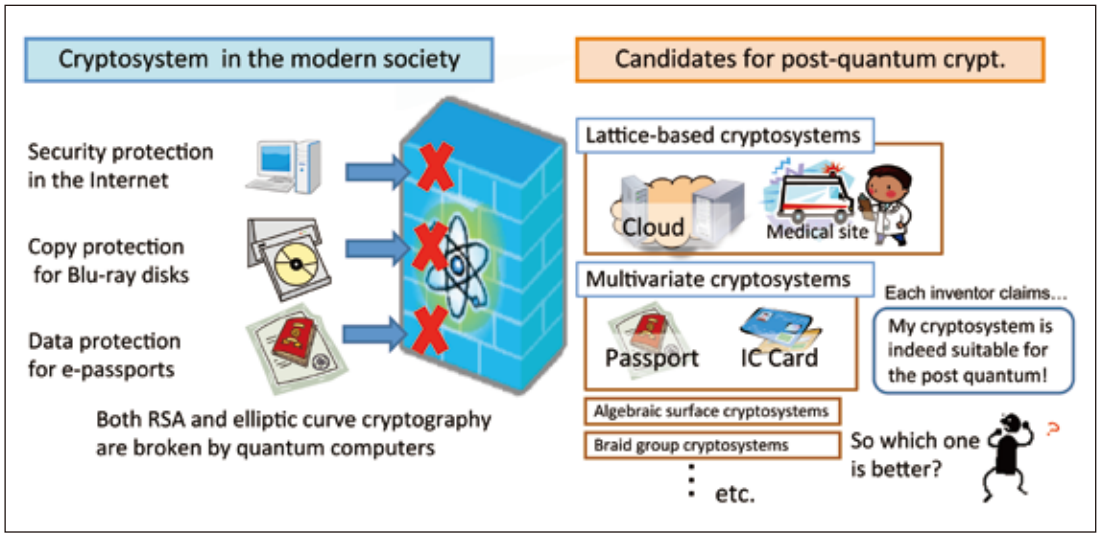


Figure 1 Our research activity helps decide which cryptosystem is the de facto standard of post-quantum cryptography

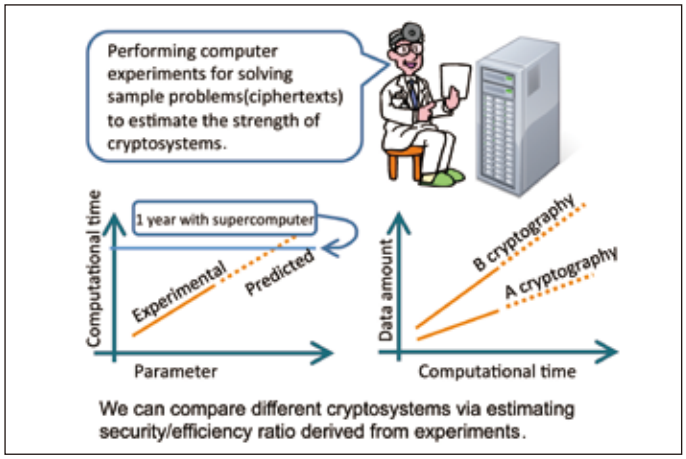


Figure 2 Computer experiments for comparing different cryptographic schemes

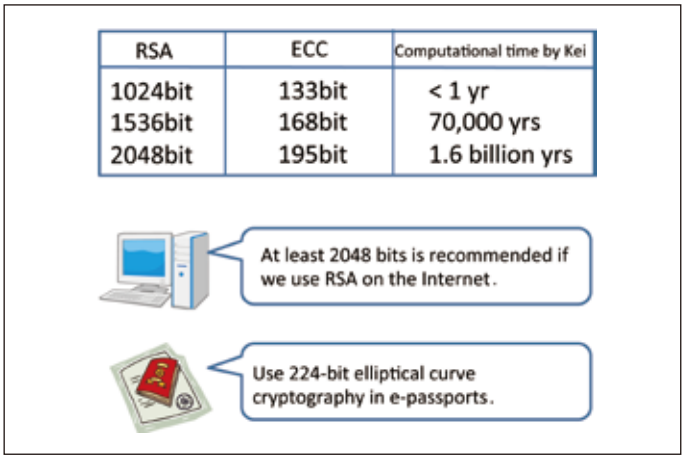


Figure 3 Comparison of RSA and ECC from experiments for setting recommended parameters

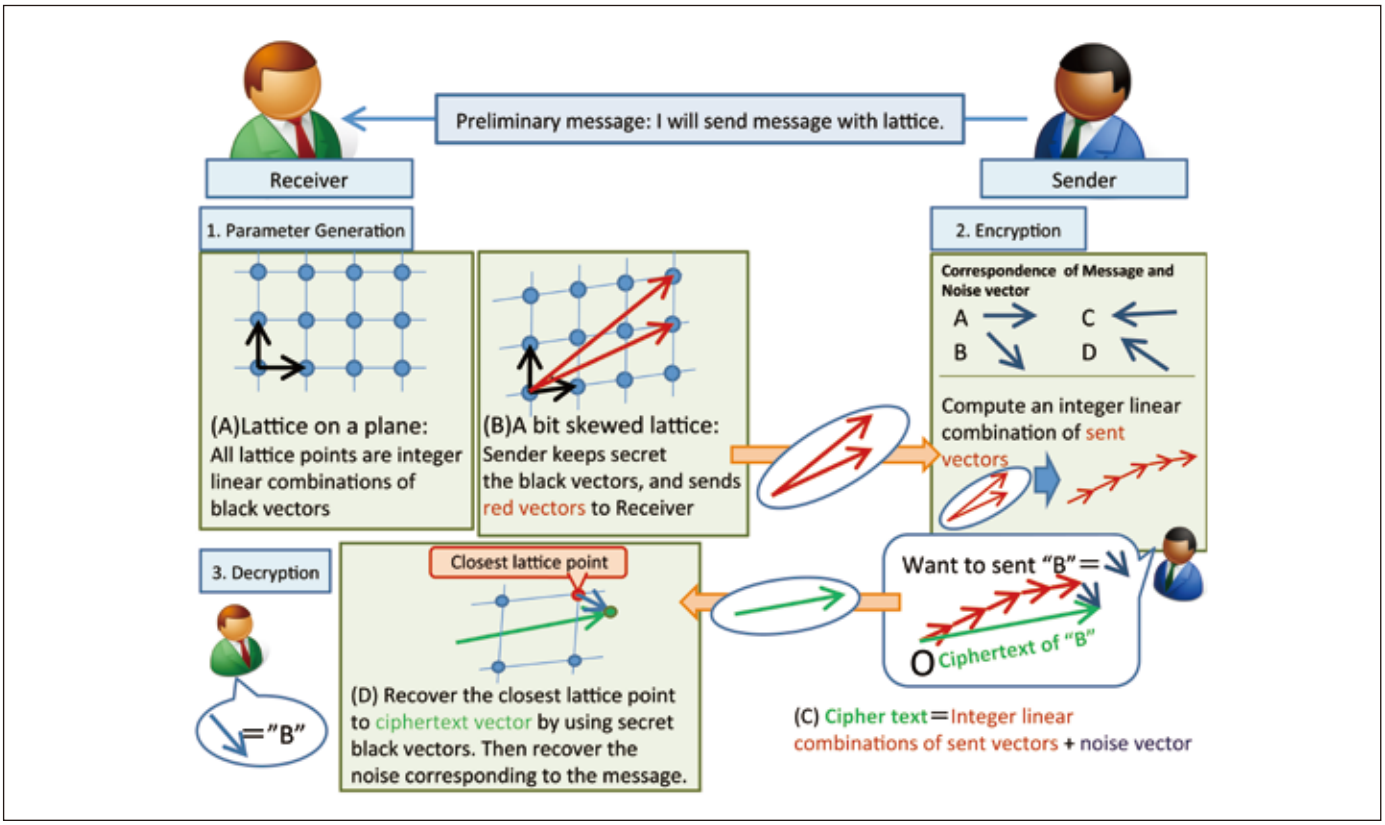


Figure 4 Outline of lattice based cryptography

Brief description of lattice-based cryptography

Figure 4 shows an outline of a lattice-based cryptography. *A lattice* is a set of points in a Euclidean space, and it is represented by a set of vectors of which all integer linear combinations are equal to the set of points, when we treat the lattice in computers. Here, (A) and (B) in the figure shows examples in the two-dimensional space. The black arrows are the set of vectors.

The communication using a lattice-based cryptography between two persons, the Sender and the Receiver, consists of three steps: 1) generating lattice parameters, 2) encrypting the message, and 3) decrypting the ciphertext.

(1) After the Sender's request for starting communication, the Receiver generates a set of nearly orthogonal vectors (represented by the black arrows in (B)). Then the corresponding lattice is also slightly skewed. Next it needs to send the data representing this lattice to the Sender. However, because the vector set (black) can be used to decrypt the ciphertext, this information must not be sent directly since the eavesdropper could recover the message, too. Alternatively, the Receiver sends a transformed vector set that represents the same lattice and cannot be used for decryption; the red vectors in (B) are an example of such set. It is known that if the vectors are nearly parallel, the set has such properties in which it cannot be used for decryption.

(2) Using the received vector set, the Sender computes an integer linear combination of the vectors; from the property of lattice, the combined vector is a point of Receiver's lattice. The encrypted data is the sum of this vector and the vector corresponding message ((C) in Figure 4).

(3) Finally, the Receiver decrypts the vector of ciphertext as follows: compute the nearest lattice point of the vector by using a set of nearly orthogonal vectors, and recover the vector of message ((D) in Figure 4).

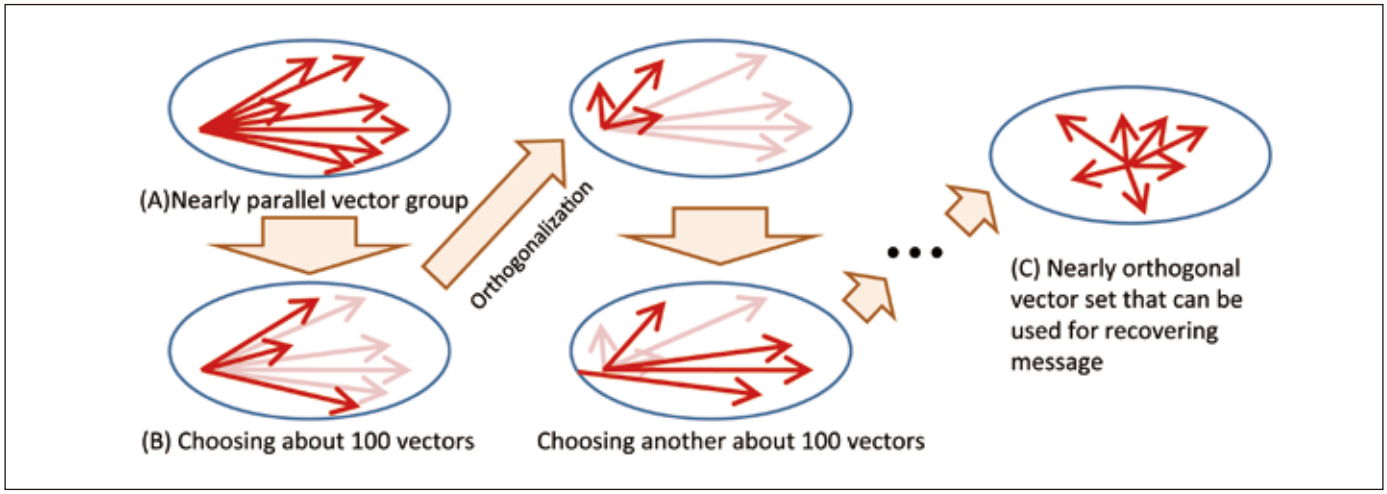


Figure 5 Outline of an algorithm for translating a vector set

Security of lattice-baced cryptography

To recover the vector corresponding to a message, it needs to find a lattice point closest to the given vector. As in step (3), the computation is easy if one has a set of nearly orthogonal vectors. On the other hand, the researchers expect that a large amount of computations are required if one only has a nearly parallel vector set. Hence, it is also expected to be hard to recover the message if an eavesdropper gets a set of nearly parallel vectors and encrypted vectors. The security of lattice-based cryptography is based on this hardness.

Consider a situation where the eavesdropper recovers a set of a nearly orthogonal vector set from the obtained set. He/she can decrypt any ciphertext encrypted with the nearly parallel vector set which is not secure. Thus, the parameters in the lattice-based cryptography must be chosen so that this recovering computation is not possible in feasible resources. Several researchers have shown that such computation is possible if the number of vectors is less than about 800, which will continue to increase in the future.

Our computer experiments based on an improved algorithm

In order to update the practical hardness estimation of lattice-based cryptography, we improved the latest algorithm and conduct our computer experiments. Recovering a nearly orthogonal vector set from a given nearly parallel vector set is known as quite a difficult problem. Performing this task is not easy with normal resources such as a desktop computer or small computing server. To solve this problem, the latest algorithm transforms the vector set step by step. Figure 5 shows an outline. First, pick a set of about 100 vectors from given set, transform it to a nearly parallel set, and finally merge the transformed set and the remaining set. Repeating this operation, the entire vector is transformed to a nearly orthogonal set.

It is known that when the vector set is nearly orthogonal, the included vectors are short as (C) in Figure 5, respectively. Hence, the above recovering problem relates to the problem of finding a short vector by transforming the vector set. The latter problem is called *the shortest vector problem of lattice*, and is also linked to the security of lattice-based cryptography. Technische Universität Darmstadt holds a contest* in which participants challenge lattice based cryptography with published sample problems of the shortest vector problem. Researchers around the world are competing in solving these problems by their algorithms and computing resources. As one of research activities in the Security Fundamentals Laboratory, we participated in the competition using the algorithm that is improved from the latest algorithm, whose number of chosen vectors is fixed. We proposed the method to give an optimized value of the number and improve the algorithm. Using our new algorithm, we established a new world record in the 825 dimensional problem.

Future work

Currently, major algorithms for analyzing the security of lattice-based cryptography are working with a small amount of memory, whereas they require a large amount of time. On the other hand, it has been known that a general property of algorithms, called *space-time tradeoff*, which is roughly speaking, increasing memory amount makes the computation faster (Figure 6). We expect to create a new faster algorithm by using this property and to evaluate the shortest vector problem again. Moreover, the above algorithm that recovers a nearly orthogonal vector set can be used for analyzing not only lattice-based cryptography, but also for other cryptosystems. Updating the known results for these cryptosystems is also in our future activities.

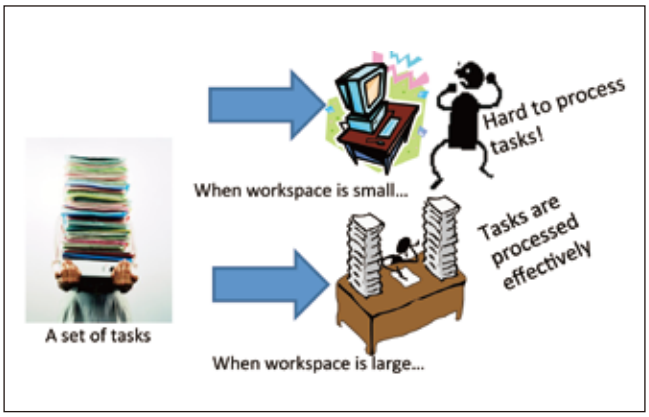


Figure 6 Concept of space-time tradeoff

* TU Darmstadt Lattice Challenge, is the contest in which participants attempt to solve the shortest vector problem that has been held by Technische Universität Darmstadt since 2008. To estimate the practical hardness of lattice based cryptographic schemes, researchers from around the world are making efforts to solve the sample problems, which are of 500 to 2000 dimensions in 25 steps.

Cryptanalysis and CRYPTREC Ciphers List Revision

Security Fundamentals Laboratory, Network Security Research Institute

Contributions to CRYPTREC

CRYPTREC, short for Cryptography Research and Evaluation Committees, is a project that monitors and evaluates the security of ciphers published on a cipher list (e-Government Recommended Ciphers List) that should be referenced for procurement in Japan's e-government. It also reviews and investigates appropriate implementation and operation procedures of cryptographic technology. CRYPTREC includes a cryptographic technology investigative commission that is co-run by Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry and also three sub-commissions co-run by NICT and Information-technology Promotion Agency, Japan (IPA). In CRYPTREC, the Security Fundamentals Laboratory has monitored ciphers published thus far in the e-Government Recommended Ciphers List and played an important role in providing necessary technical advice as security deteriorates with age. The e-Government Recommended Ciphers List, first published in 2003, was revised in accordance with recent technological developments, and released on March 2013 by the Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry as CRYPTREC Ciphers List. The Security Fundamentals Laboratory contributed to this revision work in cryptographic security evaluations and head office operations.

CRYPTREC Ciphers List revision

Although the e-Government Recommended Ciphers List was selected in 2003 from the standpoint that its ciphers could be safely used for 10 years, in 2013, the "CRYPTEC Ciphers List", a revised version of the "e-Government Recommended Ciphers List" was created* due to the facts that: (1) 10 years had passed; (2) security had become weaker due to advancements in cryptanalysis technology and computers; and (3) cipher usage had expanded. The CRYPTREC Ciphers List not only examines from the standpoint of security but various other aspects, such as procurement practicality and domestic cipher promotion, and includes the "e-Government Recommended Ciphers List", "Candidate Recommended Ciphers List", and "Monitored Ciphers List". Cryptographic technologies whose security and implementation performance have been confirmed are published in the e-Government Recommended Ciphers List and Candidate Recommended Ciphers List. In particular, ones in which procurement in CRYPTREC has been determined as practical are published in the e-Government Recommended Ciphers List (Figure 1). In addition, the Monitored Ciphers List lists cryptographic technologies that have lost their recommendation status such as Hash Function SHA-1 because the actual risk of being decoded is high, among others reasons.

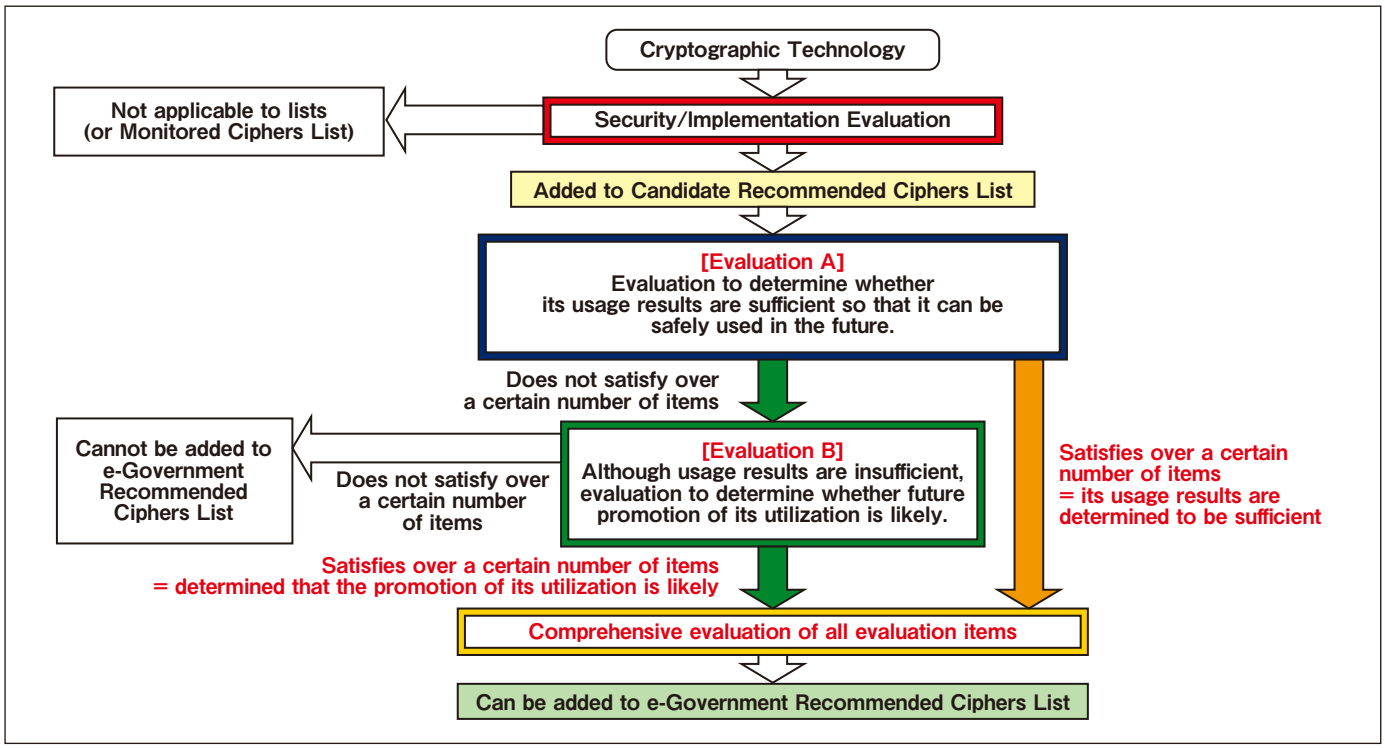


Figure 1 List revision process

* List of ciphers that should be referenced for procurement in e-government (CRYPTREC Ciphers List)
http://www.soumu.go.jp/main_content/000206523.pdf

Awards

Recipient(s) ● MATSUO Shin'ichiro / Director of Security Architecture Laboratory, Network Security Research Institute

Co-recipients:
MIYAZAKI Kunihiko (Hitachi, Ltd.)
OOTSUKA Akira (The National Institute of Advanced Industrial Science and Technology)

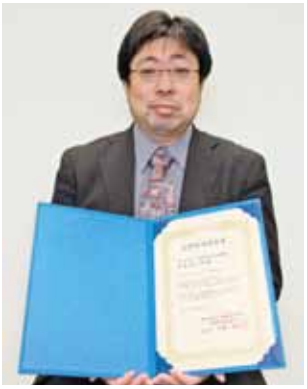
◎Award Date: March 19, 2012

◎Name of Award:
International Standards Development Award

◎Details:
For editing ISO/IEC29128 (First Edition) Verification of Cryptographic Protocols as a co-editor in ISO/IEC JTC1 and completing publication of the ISO.

◎Awarding Organization:
Information Technology Standards Commission of Japan

◎Comment from the Recipient(s):
Recently, we have completed the standardization of security verification methods of security technology in ISO/IEC JTC1. When we use networks, we also use many security technologies as well. It is necessary to verify whether or not these technologies are actually protecting us. This standard gives a measurement in validation. I am grateful to all those who helped support this standard and hope to continue contributing to the dissemination of NICT research results in the future.



Recipient(s) ● Ganesh Gowrishankar / Research Expert, Brain ICT Laboratory, Advanced ICT Research Institute
(Present: Researcher, Brain Networks and Communication Laboratory, Center for Information and Neural Networks)

Co-recipients:
Chenguang Yang, Sami Haddadin, Sven Parusel, Alin Albu-Schäeffer, and Etienne Burdet

◎Award Date: May 17, 2012

◎Name of Award:
2011 King-Sun Fu Memorial IEEE Transactions on Robotics Best Paper Award

◎Details:
This award, presented (once a year) for outstanding papers that reflect the purpose of IEEE Transactions on Robotics, was received in recognition of the paper's technical aspect, originality, potential impact, clarity of presentation and its practical significance for application.

◎Awarding Organization:
IEEE Robotics and Automation Society

◎Comment from the Recipient(s):
My research interest lies in understanding the computational processes behind human motor abilities and utilizing this understanding to develop flexible motion control and learning in robots. My research believes that integrated research in robotics and motor neuroscience is a promising way forward for both of these fields. This 'Best paper award' (which is one of the most prestigious yearly robotics award in the world) is in regard to one such project where we investigated the human abilities to adapt their limb trajectory, forces and impedance during interaction with the environment and implemented them in robots to achieve similar intelligence in robots.

Recipient(s) ● NARUSE Makoto / Senior Researcher, Photonic Network System Laboratory, Photonic Network Research Institute

Co-recipients:
TATE Naoya, The University of Tokyo
SEKINE Yoko; HOGA Morihisa; OHYAGI Yasuyuki, Dai Nippon Printing Co. Ltd.
MATSUMOTO Tsutomu, Yokohama National University
OHTSU Motoichi, The University of Tokyo

◎Award Date: July 24, 2012

◎Name of Award:
26th (2012 FY) Grand Prize for Advanced Technology Leading in Originality
Outstanding Performance Award (FujiSankei Business *i* Award)

◎Details:
Research and development of nano-photonic security that uses nano-scale light.

◎Awarding Organization:
FujiSankei Business *i*

◎Comment from the Recipient(s):
I am deeply grateful to all those involved who led us to receive such a traditional and distinctive award. The research subjected to this award is about the realization and principles of light systems using "small light" called an optical near-field. NICT, The University of Tokyo, Dai Nippon Printing Co., Ltd., and Yokohama National University jointly conducted system design, nanostructure fabrication, optical near-field analysis, and performance evaluation. The awards ceremony was conducted in the presence of Princess Hisako Takamado, and I was much honored to give a panel exhibit explanation. Thank you for your continued guidance.

Second from the left: NARUSE Makoto

Recipient(s) ● KOJIMA Fumihide / Senior Researcher, Smart Wireless Laboratory, Wireless Network Research Institute

◎Award Date: July 31, 2012

◎Name of Award:
The IEEE Standards Association acknowledge with appreciation

◎Details:
For outstanding contributions to the development of IEEE Standard 802.15.4e-2012; IEEE standard for local and metropolitan area networks- Part 15.4: LR-WPANs, Amendment 1: MAC sublayer

◎Awarding Organization:
IEEE-SA
Technical Committee on Satellite Communications

◎Comment from the Recipient(s):
With this achievement, which developed power-saving radio technology for smart-meters—desired by domestic gas companies and meter makers—as an international standard thanks to NICT contributions, I realized the great significance from NICT's part as contributor to the development of domestic communications technology and am extremely honored in receiving this award. This technology field is currently in a post-standardized, diffusion phase, and I hope to continue making proper contributions as NICT to its future development.

Recipient(s) ● ISAWA Ryoichi / Researcher, Cybersecurity Laboratory, Network Security Research Institute

◎Award Date: September 5, 2012

◎Name of Award:
FIT2011 Young Researcher Award

◎Details:
In recognition of the distinguished paper, titled "One-Time Password Authentication Scheme to Solve Stolen Verifier Problem"

◎Awarding Organization:
Information Processing Society of Japan

◎Comment from the Recipient(s):
I am extremely happy to have been able to receive this award. In FIT2011, I proposed a one-time password authentication scheme for a client and server to securely verify one another. The proposed scheme's feature that was praised was its tolerance against "hybrid theft attacks" where an attacker steals information from a server or communication channel and spoofs his/her identity. I would like to thank all those whom I engaged in beneficial discussions with on this research.

Recipient(s) ● FUJIEDA Miho[*i] HACHISU Hidekazu[*ii] LI Ying[*i] KUMAGAI Motohiro[*i] NAGANO Shigeo[*i] IDO Tetsuya[*iii]

*i Senior Researcher, Space-Time Standards Laboratory, Applied Electromagnetic Research Institute
*ii Researcher, Space-Time Standards Laboratory, Applied Electromagnetic Research Institute *iii Planning Manager, Strategic Planning Office, Strategic Planning Department

Co-recipients:
YAMAGUCHI Atsushi
(Physikalisch-Technische Bundesanstalt)
TAKANO Tetsushi, TAKAMOTO Masao, KATORI Hidetoshi
(The University of Tokyo)

◎Award Date: September 11, 2012

◎Name of Award:
The Japan Society of Applied Physics Academic Paper Award (Outstanding Paper Award)

◎Details:
For the outstanding paper on the direct comparison of Sr optical lattice clocks using an NICT-The University of Tokyo optical fiber link, titled "Applied Physics Express Vol. 4 082203 (2011)"

◎Awarding Organization:
The Japan Society of Applied Physics

◎Comment from the Recipient(s):
There has been a demand in recent years to redefine the SI second with optical frequency standards, but due to lack of means to verify the accuracy of optical frequency standards, it still has not been implemented. In this paper, we established a comparison means through optical fiber and confirmed the coincidence between two Sr clocks with an uncertainty of 10^{-16}. It is a great honor for our results—from everyone working together and many work-filled nights—to be recognized. We would like to thank everyone for their support including the usage of the optical test bed, JGN2plus.

From left: KUMAGAI Motohiro, YAMAGUCHI Atsushi, IDO Tetsuya, HACHISU Hidekazu, FUJIEDA Miho, LI Ying

Recipient(s) ● OKAMOTO Takuma / Researcher, Multisensory Cognition and Computation Laboratory, Universal Communication Research Institute

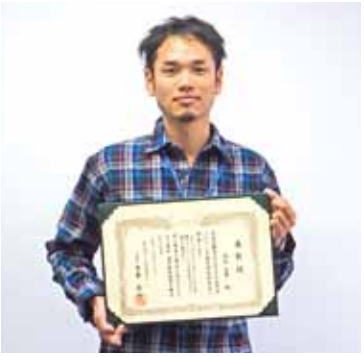
◎Award Date: September 20, 2012

◎Name of Award:
Awaya Prize Young Researcher Award

◎Details:
Improvement of masking signals for acoustic privacy area generation using a multichannel loud-speaker array

◎Awarding Organization:
The Acoustical Society of Japan

◎Comment from the Recipient(s):
The Awaya Prize Young Researcher Award I received is bestowed upon young researchers by evaluating not only one particular presentation but their comprehensive achievement. I take this award as an incentive to continue research into the future. Using a number of speakers, I proposed a method that generates an area where speech sound can be heard and another area where nothing can be heard. In the future, I hope to develop this method not only for speech privacy but also as ultra-realistic acoustic communication technology in which one can hear different sounds in various locations.



Recipient(s) ● SASAKI Kensuke / Researcher, Electromagnetic Compatibility Laboratory, Applied Electromagnetic Research Institute

◎Award Date: September 20, 2012

◎Name of Award:
The Institute of Electrical Engineers of Japan Outstanding Paper Presentation Award

◎Details:
For a presentation in FY 2011 (authors: SASAKI Kensuke, WAKE Kanako, WATANABE Souichi) at The Institute of Electrical Engineers on basic/material/common sections being recognized as an outstanding paper presentation.

◎Awarding Organization:
The Institute of Electrical Engineers of Japan

◎Comment from the Recipient(s):
Our research presentation in the area of electromagnetic field theory was recognized and we received the Outstanding Paper Presentation Award. In this research, we proposed and examined exposure assessment technology for human bodies in millimeter waveband, which was formerly considered difficult. I would like to thank the Electromagnetic Compatibility Laboratory and everyone involved for their continuous support and advice during our pursuit of the research.

Report on Space Weather Users' Forum

ISHII Mamoru, Space Weather and Environment Informatics Laboratory,
Applied Electromagnetic Research Institute

On February 26, 2013, we held the Space Weather Users' Forum in the International Conference Room, 4th floor of Building 1 at NICT headquarters. The event was a huge success reaching almost full capacity with over 90 participants from public offices, universities, research institutes, and aviation and satellite operations fields. The Forum, which began with a greeting from KUMAGAI Hiroshi, Vice President, Member of the Board of Directors, consisted of two parts. In the first part, ISHII Mamoru, Director of NICT Space Weather and Environment Informatics Laboratory, held a lecture where he explained the current state of space weather and talked about NICT's space weather efforts. In part two, lectures were held on topics related to space weather in recent years that included: Professor CHO Mengu, Kyushu Institute of Technology, on the impact of space weather on artificial satellites, SAITO Susumu, Electronic Navigation Research Institute, on the impact of space weather on air navigation recently using satellite positioning, and MINAMOTO Yasuhiro, Kakioka Magnetic Observatory, Japan Meteorological Agency, on the impact of immense Geomagnetically Induced Current(GIC) that flows during high solar activity.

During the general discussion following the lectures, we received many questions and comments from the participants. There was much active discussion at the Forum, particularly in aviation-related matters, regarding the significance of space weather information in ICAO: International Civil Aviation Organization that is being explored due to errors in satellite positioning information mainly caused by ionospheric fluctuations even though the use of this information is being promoted for air navigation systems. Many audience members also expressed strong interest in the impact of Geomagnetically Induced Current (GIC) on electric power facilities which were previously thought to be insignificant; the result stated that reexamination is necessary depending on advancements of future research.

After the Forum, more than 30 participants visited the Forecast Room where the Space Weather Forecast Conference at NICT is held. With a large number of participants receiving daily space weather forecast information via email, many expressed that they were glad they had a chance to visit the actual site where the forecasts are conducted. We also learned that there are high levels of interest and anticipation towards our space weather forecasts through the survey in which participants wrote what they thought about each lecture, including "easy to understand" and "completely understood." We hope to further improve in the future with what we learned about examples of different uses of the space weather information NICT provides and the many requests we received.

Scene of a lecture

Participants visited the Space Weather Forecast Room

NICT Entrepreneurs' challenge 2 days
“Kigyouka Koshien” and “ICT Venture Business Plan Contest”

NICT provides support towards business expansion of community-based venture businesses in the field of ICT and the cultivation and discovery of next-generation talent from technical college, university, and graduate school students around the country who aspire to become involved in businesses that utilize ICT.

As part of this effort, we held “the Kigyouka Koshien” for young people and students to compete with their business plans and“the ICT Venture Business Plan Contest” where promising venture businesses from around Japan compete with their business plans as well, promoting business-matching such as fund-raising and market expansion.

(Please see the next page for details on the ICT Venture Business Plan Contest.)

Report on The 2nd Kigyouka Koshien

Thursday, March 7, 2013

Cyber Agent Ventures, Inc. Startup Base Camp (Akasaka, Minato-ku)

Presentations were held by 9 teams selected from all around Japan, and in addition to the highest award and special review committee award, other “Special Awards” were bestowed such as one which grants recipients the privilege to participate in internships provided by 13 supporting businesses. At the exchange event, lively exchanges ensued with participation from approximately 100 supporting businesses and affiliates.

Highest Award

Team☆Hitoride dekirumon (HORIUCHI Kohei, Representative), The University of Electro-Communications
“Code-Reading Platform ‘CodeLibrary’ that Will Change the Self-Learning Culture Among Engineers”

This is a social code-reading platform that reads open source (OSS) code and improves technological capabilities in your free time. This platform essentially provides applications for free and earns profit from the margin of traded know-how linked to code between users on the platform.

Jury's Special Award

ShinBunet (KANESHIRO Shun-Ichiro, Representative), Okinawa National College of Technology
“ShinBunet”

This is a system for resolving the information gap (digital divide) of people who cannot use the Internet. It automatically collects information from the Internet by holding your hand over a newspaper article of interest and displays it on an iPad. When displayed on the iPad, it aims to monetize by embedding advertisements in a newspaper layout. Also, because we can collect data on what related information newspaper subscribers want for which articles, linking other business opportunities using this data is also possible.

Glimpse of the venue

Commemorative photograph after the presentation ceremony

NICT Entrepreneurs' challenge 2 days "Kigyouka Koshien" and "ICT Venture Business Plan Contest"

Report on The ICT Venture Business Plan Contest FY2012

Friday, March 8, 2013

WTC Conference Center (Hamamatsu-cho, Minato-ku)

After the Highest Award-winning team of "Kigyouka Koshien", held on the preceding day, gave a presentation and NICT Outcome Promotion Department introduced their efforts of intellectual property and technology transfer, eight venture businesses gave presentations, and the grand prize as well as the Audience Award newly established this year were awarded based on audience votes. With approximately 200 participants that day, there was much lively exchange of opinions and business talk at the information-networking event after the program.

(Please see the previous page for the details on the Kigyouka Koushien.)

Grand Prize

GClue Inc. (SASAKI Akira, President)
"iOS-Linked Hard Platform"

The team aims to construct a platform centered around iOS-linked hardware that is developed as open source hardware, release the developed iOS-linked portfolio as open source and open source hardware and develop its kit sales and kit-generation courses. Its first target is to make an iOS-linked toy and develop a toy market that allows collaboration with the iPhone as Open Source Omocha (oSo).

Audience Award

REEVO Inc. (MATSUO Ryoma, President & CEO)
"Provision of the Compact Electric Car Sharing System, 'codekake'"

A uniquely developed car sharing system for compact electric automobiles (1-2 seats) attracting attention as new mobility. This system's three features are: (1) you can complete required procedures such as member registration, license verification, vehicle reservations, toll payment, etc. all within a smartphone application; (2) supports one-way usage between stations; and (3) can connect with the installation-point and provide customization by adding functions such as sightseeing route directions and local area voice guidance to the in-vehicle display and smartphone applications.

Presentation scene

Glimpse of the venue

Commemorative photograph after the awards ceremony

Information for Readers

The next issue will feature a strontium optical lattice clock becoming the forefront of optical frequency standards and new research projects.

NICT NEWS No.426, MAR. 2013
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/en/data/nict-news/

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/en/