4 Security Fundamentals Technology

4-1 Research Activity on Security Fundamentals Technology

TANAKA Hidema

In this paper, we show the activity of research between 2006 and 2010 on security fundamentals technologies.

Keywords
Security fundamentals technology, Cryptography, Mathematics, Electromagnetic emanation

1 Introduction

The Security Fundamentals Group was formed as one of the groups which constituted the Information Security Research Center when the Research Center was established in January 2005, on the basis of the Emergency Communications Group, and thus the Security Fundamentals Group started its activities even before the second medium-term plan period. While the group configuration of the Information Security Research Center was altered in April 2006 when the second medium-term was started, the Security Fundamentals Group is the only group whose name and staff members were not changed. The Group has continued its activities as the Security Fundamentals Laboratory also during the third medium-term plan period which started in FY2011. Because its research focus, cryptographic technologies, is quite essential to ensure the security of the communications infrastructure, continuous activities are most important to maintain security. For NICT whose objective is to ensure the safety and security of communications in the nation, maintaining the Security Fundamentals Group is fundamental for its activities.

The Group's operational characteristic is its small number of staff members. The number of regular staff members has been only two during most periods while it was three at maximum only in FY2010. The maximum number of staff members including part-time contract researchers was 13, and about half of the budget was used for personnel expenses. Because, as one of the staff members' characteristics, the Group's main members joined activities when the Cryptography Research and Evaluation Committees (CRYPTREC) were started, the Group has maintained the continuation of the evaluation of e-government recommended ciphers. The CRYPTREC, which is detailed in [1] is a joint project of the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry, and its head office was placed in NICT and the Information-technology Promotion Agency, Japan (IPA); therefore, the Group has conducted cross-ministry activities from the beginning. This had made discussions, etc., complicated and caused the staff members to spend a lot of time on meetings not directly related to research activities. Furthermore, although the security of cryptography needs multifaceted evaluation, such problems as differences in researchers' specialties and shortage of man-

power were encountered.

The Group occasionally faced such difficult problems that it had to set up cryptography research themes which could lead to academic significant activities and that it had to give explanations which are easy to understand for general people. Because policies, visions, and evaluation can vary widely, depending on the situation, the Group might not give coherent explanations for the same activities in some cases, for example, during the second medium-term plan period. However, it can be said that the Group managed to conduct research activities under coherent policies. For example, although the CRYPTREC engaged in complex cross-ministry activities as aforementioned (not merely operation of the head office), its activities started to draw great attention due to occurrence of cryptography vulnerability problems and due to ministries' cryptographic-technology transition plans in around 2007; and the deployment of the research results and the CRYPTREC were linked and evaluated, making the staff members feel that their efforts were rewarded.

Because the Group's research is centered on mathematical algorithm research, it was always difficult to give clear explanations about its research. Technical review and understanding must come before explanation to general people is considered, and thus it is very dangerous to formulate research policies, without taking it into consideration. This is not a problem of the Group, rather a problem to be solved about how independent administrative institutions' policies should be determined and how their activities should be explained. The Group suggests that polices be shifted from those shared by the entire NICT to those which reflect characteristics of the individual research fields.

In this way, the Group's basis for activities has been relatively weak, and its management has not been smooth enough. While it is difficult to explain its research activities and to gain understanding, it was fortunate that the Group's research field needed much less budget than other activities in NICT, as mentioned later. While the Group was occasionally subjected to such a politically-incorrect view that it was overly specialty oriented, it, in practice, could have staff members who were motivated to tackle other fields and social deployment and took the trouble to contribute to the Group. This article outlines activities from FY2006 to FY2010. In Chapter **2**, the outline and achievements of each research theme are described. In Chapter **3**, the status of budget spent for the individual research themes is described. In Chapter **4**, the change of the personnel configuration is described.

2 Outline of activities

The themes of the Security Fundamentals Group's activities can be broadly classified into the five categories.

1) Mathematical structure and algorithms
2) Cryptography protocols
3) Cryptographic-technology security evaluation
4) Electromagnetic emanation security
5) CRYPTREC

While it is difficult to clearly classify actual research activities and such an attempt does not make sense, it can be said that the Group started its activities with 1) Mathematical structure and algorithms. Activities which started with mathematical structure and algorithms and which aimed to materialize new security functions lead to research which involves the research field of 2) Cryptography protocols. Activities which aimed to develop new security evaluation methods lead to 3) Cryptographic technology security evaluation. Furthermore, combinations with electromagnetic emanation measurement technologies lead to activities regarding 4) Electromagnetic emanation security. 5) CRYPTREC represents the integration of all the activities; in addition to deployment of security evaluation results, CRYPTREC has introduced new technologies, investigated the trend of new technologies, and published annual reports. On the other hand, there were cases where the Group obtained research themes through discovery of prob-

lems and discussions about e-government services during CRYPTREC activities. The revision of the guideline of the electronic signature law, the ID base cryptography, and the post quantum cryptography algorithm are some examples of such activities. The main activities are described below:

1) Mathematical structure and algorithms

The Group dealt with issues such as algebra, formal method, prime factorization, and discrete logarithm problems. As for algebra, it performed element development of cryptographic primitives and applied these to security evaluation regarding higher order differential attacks, etc. Automated theorem proving is deployed for protocol security evaluation. As for prime factorization, it estimated security evaluation regarding public-key cryptography RSA-1024. As for the discrete logarithm problem, it presented the world's best result regarding the size of the resolvable problem.

2) Cryptography protocols

The research results are diverse, and representative ones include proxy re-encryption methods, anonymous password based authenticated key exchange (APAKE), signature schemes which ensure security even when part of attribute-based encryption, homomorphic encryption, or key information is leaked, and multi-signature schemes which allow signature data structure to be kept uniform. The Group also developed, for example, quantum secret sharing schemes which assume quantum ICT.

3) Cryptographic technology security evaluation

The Group performed mainly security evaluation regarding symmetric-key cryptography. Security evaluation regarding public-key cryptography such as prime factorization and discrete logarithm is categorized as mathematical structure and algorithms due to the characteristics of the research. Here, the Group evaluated mainly 64-bit block cryptography. It also dealt with side-channel attacks and performed feasibility verification regarding fault attacks, especially. In addition, working with the Quantum ICT Group, it dealt with security evaluation regarding quantum key distribution and quantum noise secure-communication.

4) Electromagnetic emanation security

Working with the EMC Group, the Group dealt with information leakage through electromagnetic emanation, and developed technologies to handle this problem. The Group engaged in screen information leakage (TEMPEST) especially, and the developed technologies were commercialized by a venture company. In addition, quantitative evaluation methods and measurement methods of electromagnetic emanation were adopted and recommended by the ITU-T as the international standards. While the Group received high evaluation for the technologies and was called the headquarters of electromagnetic emanation security research, it ended the relevant activities at the end of 2009 when international standardization of the methods became highly likely.

5) CRYPTREC

The Group deployed the evaluation results of e-government recommended cryptographic technologies, investigated the specifications of various online services by e-governments, performed security evaluation, and supported the selection of appropriate cryptography; this is detailed in [1].

Figure 1 shows the change of number of relevant papers other than those about CRYPTREC (not pure research activities). Each of the presentations at domestic conferences and papers published in journals is counted as one without any distinction. The figure shows that in early the second medium-term plan period, the majority of the papers were written about mathematical fields which are the basis of the Group's activities, and the number of papers gradually increased concerning the results of cryptography protocols which are applications of cryptographic technologies and are related to system construction. While constant achievements were made regarding security evaluation of cryptographic technologies, researchers responsible for security evaluation bore a lot of the burden about CRYPTREC works in FY2009 (due to the change of the framework, for example), and thus the number

of relevant papers was small. Because activities concerning electromagnetic emanation security were completed at the end of FY2009 as aforementioned, no achievements were reported in this regard in FY2010.

Research themes and budget use

The Security Fundamentals Group has mainly engaged in mathematical and theoretical researches, and research achievements depend on researchers' abilities, rather than testing environments and equipment, and thus generally research achievements are not affected by the amount of budget. The budget for research activities has been mainly used for trip expenses for presentations at academic conferences. With respect to electromagnetic emanation security (experiment-centered activities), as an exception, the budget was also used for resources, equipment prototype creation, rent of anechoic chambers, and other necessities. In addition, because computer simulation needs to be performed for all the research themes, a shared server system was built up over five years. Purchase of publications is another characteristic use of the Group's budget. In five years, 4,000 publications were purchased, and movable book racks for those publications were installed. As for the management of the head office for CRYPTREC activities, about half of the annual budget has been used.

During the period while large-scale experiments were needed for electromagnetic emanation security, a larger budget was required by the Security Fundamentals Group. During other periods, the budget depended on the number of presentations and papers. That is, as the number of academic achievements increased, the trip expenses for participating in academic conferences increased. In FY2007 and FY2008, experiments and ITU-T related activities were active in terms of electromagnetic emanation security, and thus a larger amount of budget was used for electromagnetic emanation security. In FY2009 and 2010, the Group's staff members participated in ISO WG2 as editors, with respect to cryptography protocol evaluation methods.

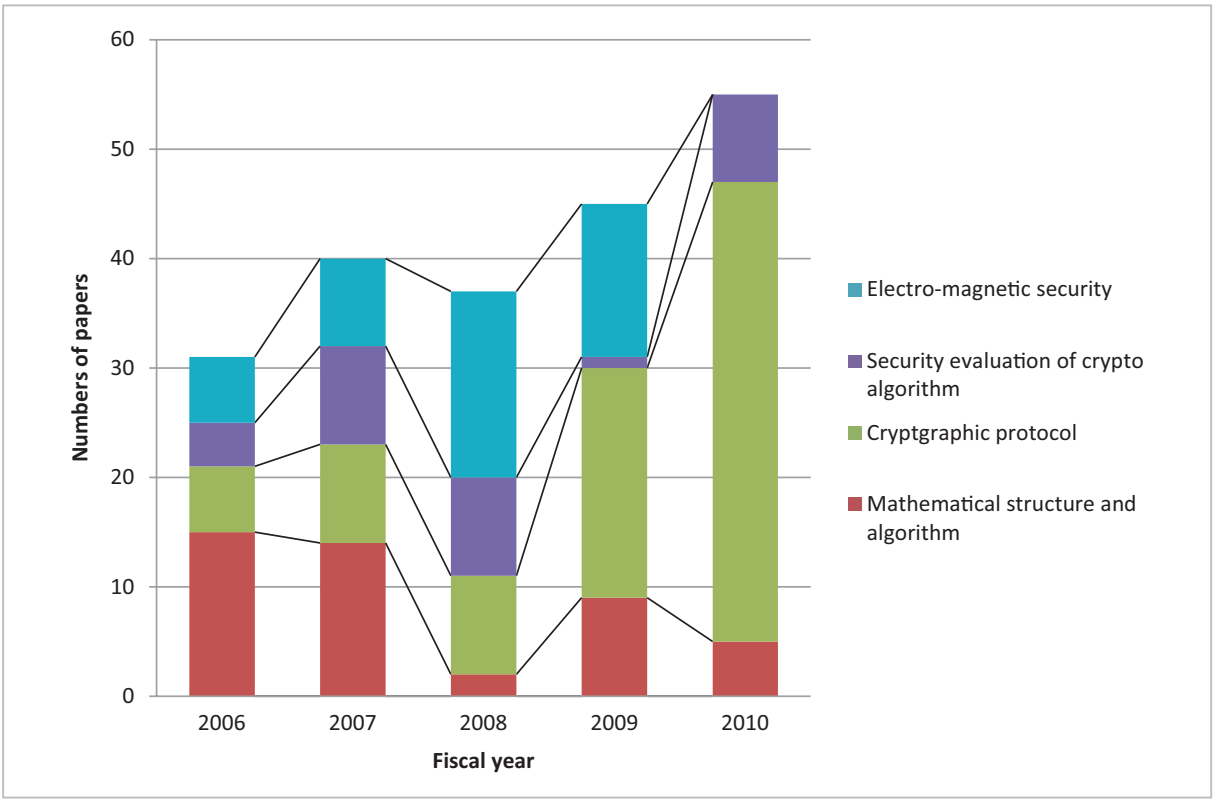

Fig.1 *Transition of the number of papers of each project*

3 Research themes and change of staff members

Figure 2 shows the change of the Security Fundamentals Group's staff members for each of the research themes. It is inappropriate to separately count the number of staff members who engaged in mathematical structure and algorithms because it is a research theme in which all the staff members involved; however, it can be said that generally achievements were made in terms of this field. Entry and departure of members in the Security Fundamentals Group was frequent, and this also happened to regular staff members and expert researchers in the middle of a fiscal year; for example, then Group Leader Dr. Yamamura moved to Akita University as a professor in May 2008. Therefore, the number of staff members was counted in April in each fiscal year.

The Security Fundamentals Group had only small number of regular staff members; only two until the end of April 2008. From May 2008 to April 2009, the Group was composed of Group Leader Dr. Takizawa (Disaster Prevention/Reduction Group) and one Chief Researcher, and in some part of these years, the Group had only one regular staff member who engaged in practical research activities. From April 2010, Dr. Tanaka worked as the group leader. As a regular staff member, Senior Researcher Dr. Matsuo joined the Group in April 2009, and Senior Researcher Dr. Okubo joined the Group in April 2010. Both of them came from private companies and greatly contributed to not only research as experienced researchers but also management of the Group and linkages with many other organizations, for example.

The average number of Expert Researchers was seven through the fiscal years. Foreign people also worked for the Group. One Chinese and one Vietnamese worked as regular staff members during the second term. In addition, one Chinese stayed for eight months as a visiting researcher.

When allocation of staff members for each of the research themes is closely examined,

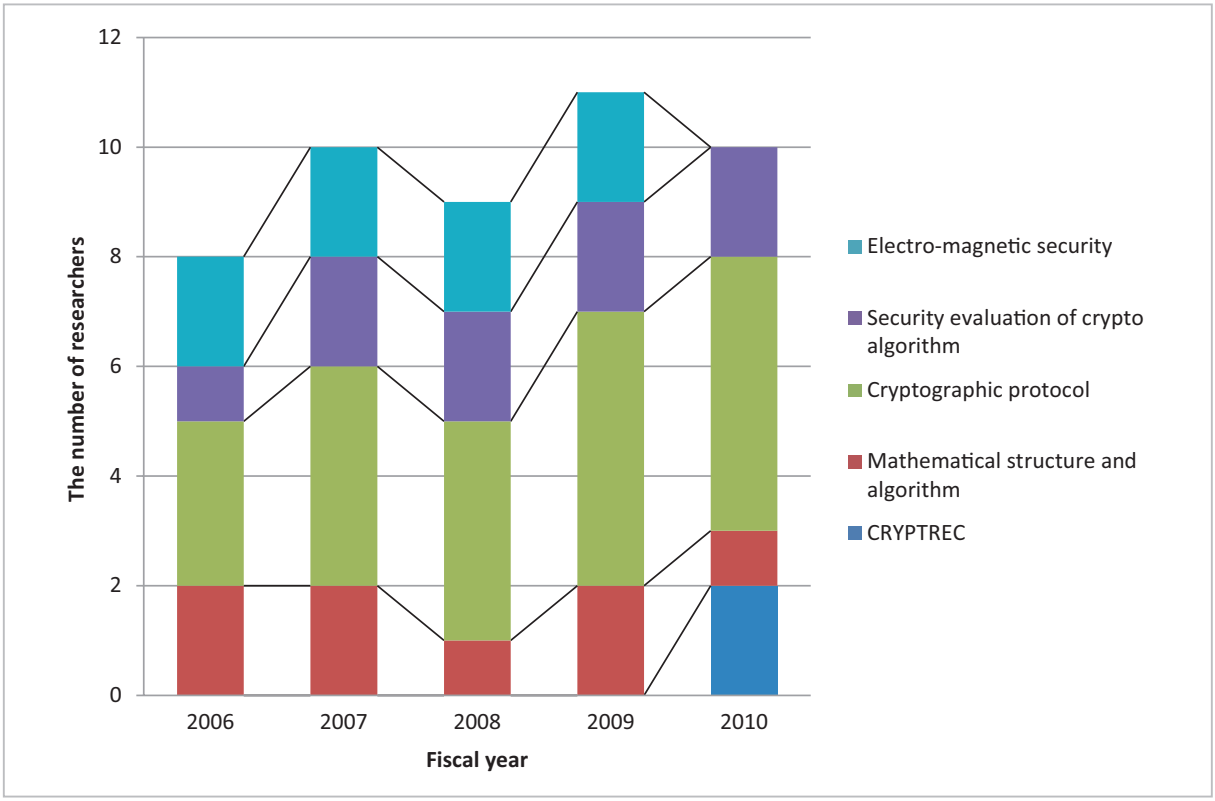

Fig.2 *Transition of the number of researchers of each project*

it will be noted that the number of members engaged in cryptography protocols gradually increased, compared with the beginning of the period. This is because, with respect to research of cryptography protocols, various sub themes were induced through combinations of security evaluation, usage, and implementability, and thus diverse personnel were needed. Also for the other themes, at least one staff member was allocated; a well-balanced configuration of manpower was attempted in terms of the cryptography research of the entire group. However, the Group had trouble with the shortage of manpower in important fields such as software/hardware implementation technologies, information-theoretical security evaluation, and quantum information theory.

4 Linkage with external institutions

The Security Fundamentals Group has also been actively engaged in activities with external institutions. During the second medium-term, it conducted activities under the following joint-research contracts:

A) Research about security evaluation regarding hash functions
The University of Electro-Communications (October 1, 2009 to March 31, 2011)

B) Research regarding evaluation of strength of cryptography protocols whose security depends on the discrete logarithm problem
Future University–Hakodate (February 9, 2009 to March 31, 2011)

C) Research regarding evaluation of strength of cryptography protocols whose security depends on the discrete logarithm problem
Kyushu University (April 1, 2010 to March 31, 2011)

In addition, the Group conducted research activities with the following universities and research institutions:

- Ibaraki University
  Professor Kaoru Kurosawa
- University of Tsukuba
  Professor Eiji Okamoto
- The University of Tokyo
  Associate Professor Noboru Kunihiro
- Tokyo University of Science
  Professor Toshinobu Kaneko
- Rikkyo University
  Professor Kazuhiro Yokoyama
  Professor Yuji Mochizuki
- Kanazawa University
  Professor Masahiro Mambo
- FUJITSU LABORATORIES LTD.
  Tetsuya Izu
- Beijing University of Posts and Telecommunications
  Licheng Wang, Lecturer
- Shanghai Jiao Tong University
  Professor Zhenfu Cao
- Columbia University
  Professor Moti Yung
- Swiss Federal Institute of Technology, Zurich School
  Professor David Basin
- Tallinn University of Technology
  Professor Ahto Buldas
- University of Padua
  Professor Antonio Assalini

5 Conclusion

On average, the Security Fundamentals Group's staff members have given presentations at academic conferences four times per year per person, and it can be said that the Group has made satisfactory academic achievements in terms of cryptography research. In addition, the Group has made practical social contributions through CRYPTREC, and conducted cost-effective activities with a limited budget. This has been enabled because individual staff members have been highly qualified as researchers and highly motivated; "the Few and the Proud".

Through activities regarding CRYPTREC, the Group had conducted a wide range of activities with the Institute for Monetary and Economic Studies of the Bank of Japan, Japan Data Communications Association, Time Business Forum, and other institutions, in terms of, for example, security evaluation of cryptographic technologies and informa-

tion provision regarding transition of cryptographic technologies. Furthermore, the Group has worked actively for international standardization; for example, Senior Researcher Dr. Matsuo worked as an editor and project manager at the ISO, and Expert Researcher Dr. Sekiguchi worked as an associate rapporteur at the ITU-T.

While cryptography research tends to lead to basic research activities, it is the Group's honor that the Group has played a significant role needed as a public research institution, taking social contribution into consideration.

Acknowledgments

We highly appreciate Akihiro Yamamura, professor of Akita University who, as the first leader, clarified the Group's policies and built the foundation for the Group's activities. We also highly appreciate the second leader Osamu Takizawa (manager) who contributed greatly to the Group while taking on a large burden by managing two groups. In addition, we have to thank R&D Advisor Te Sun Han and R&D Advisor Kingo Kobayashi, for helping us with enrichment of basic theories through, for example, opening seminars for network information theories. We also have to thank Miki Tanaka, Hidenori Sekiguchi, Junji Nakazato, Hitoshi Tamura, Tomohiro Harayama, and Shinji Seto who worked as Expert Researchers, Invited Advisor Yasuo Miyagawa, and Group Assistant Makiko Shimizu; all of them contributed greatly to the Group.

References

1 Takashi Kurokawa and Sachiko Kanamori, "CRYPTREC Activities," Special issue of this NICT Journal, 4-9, 2011.

(Accepted June 15, 2011)

TANAKA Hidema, *Ph.D.*

Director, Security Fundamentals Laboratory, Network Security Research Institute

Information Security, Cryptographic Technology, Information Theory