Advanced Concept of Information Security Comprehensive Science

Shigeo Tsujii, Hiroshi Yamaguchi, Masahito Gotaishi, *Research & Development Initiative, Chuo University, Kasuga, Bunkyo, Tokyo, Japan, Email: tsujii@tamacc.chuo-u.ac.jp; yamaguchivc@cap.ocn.ne.jp; gotaishi@tamacc.chuo-u.ac.jp*

doi: 10.22545/2014/00046

Information security and ethics as bases of our life are becoming in-creasingly important in the new information society which we have never experienced before. In this paper, we present an advanced con-cept of information security in terms of comprehensive science. Free-dom, Security and Privacy are the three key values of information soci-ety. These three values are liable to conflict with each other and among them, sometimes three contradictions arises. We use the concept of "Aufheben," (sublate), a technical term of philosophy, to cope with it. S. Tsujii introduced a new concept of information security as the com-prehensive science in 1993. Moreover, we have endeavored to evaluate the effectiveness of the concept by establishing the "MELT UP Forum." The MELT UP Forum aims to foster, to identify and to extend a core or comprehensive science that deals with Management, Ethics, Law, and Technology across a wide spectrum of endeavors.

Keywords*:* Verification, privacy, software, legal documents, logic cryptosystem.

1 Introduction

Many of you have recognized feasibility that now is the time to start a new professional society to foster, to identify and to extend a core of science that deals with a comprehensive science across a broad spectrum of human, technological and economic endeavors. A spectrum that covers the traditional disciplines of communications, computer sciences, engineering, economics, management, manufacturing, mathematics, statistics and physical social sciences. A cross disciplinary science that can deal with rethinking, reshaping and reconstructing a rapidly ever-changing world order. A world which deals with creativity and innovation to enhance shared prosperity and social and cultural enrichment. In this paper, we present an advanced concept of information security in terms of comprehensive science. Freedom, Security and Privacy are the three key values of information society. These three values are liable to conflict with each other and among them, sometimes three contradictions arises. We use a German word "Aufheben," which has a meaning of "to lift up," or "to sublate." "Aufheben" unifies values contradicting each other progressively through a process of opposition and struggle and finally lift up these three values for a higher stage. In order to achieve the meaning of "Aufheben." S. Tsujii introduced a new concept of information security in terms of comprehensive science in 1993 [5], [6], [7]. Moreover, we have been struggling to evaluate the effectiveness of his concept by establishing a new forum named "the MELT UP Forum." The MELT UP Forum aims to fosters, to identify and to extend a core of comprehensive science that deals with Management, Ethics, Law, and Technology across a wide spectrum of endeavors.

To cope with the advent of new information society, information security and ethics as bases of our life are becoming increasingly important .We are now beginning to live in a new information society which is symbolized by the four keywords, namely Social, Mobile, Cloud and Smart. We have never experienced before and we are not yet accustomed in this new world. In this paper, we present an advanced concept of information security in terms of comprehensive science. Freedom, Security and Privacy are key values of information society. These three key values are liable to conflict with each other and among them. We use a German word "Aufheben," which has a meaning of "to lift up," or "to sublate." "Aufheben" unifies values contradicting each other progressively through a process of opposition and struggle and finally develop three values: Freedom, Security and Privacy for a higher stage. For achieving "Aufheben" function, we introduce a new concept of information security in terms of comprehensive science which was proposed by S. Tsujii in 1993. An idea of tightly coupled co-operation scheme named "the MELT UP Forum" is introduced.

1.1 Structure of the Paper

This paper is structured as follows. First we propose the concept of the information security as the science to sublate the irrationality of the "contradicting requirements." In the chapter 2 and 3, the technologies to overcome the contradiction, organization cryptosystems and logical cryptosystems, are described. And finally, the necessity of inter-disciplinary science and human resource development is discussed in the chapter 4. The overall points are summarized in the chapter 6.

1.2 Philosophy and concept of information security

Generally implementation of the information security requires not only the technical knowledge but also the business, law, politics or psychology. One of ultimate basics would be the ethics and discussing what is right and what is wrong. It would require the discussion based on the humanities, philosophy and psychology. Therefore the information security is formed with a comprehensive science. Freedom, Security, Privacy– these three key words seems to summarize the ideal of the IT society. According to Hegel, a German philosopher, he explained "History is the process of broadening freedom." It is certain that the law of history as defined by Hegel applies to the present day in spite of the historical and geographical distances. We can freely expanded from "Physical Space" to "PhysicalCyber Space". In the majority of the cases the compromise between the two has been sought for. However, Tsujii has claimed that the contradiction should be overcome by "sublation."

A new world that human beings have stepped into for the first time. In the new world, they have acquired greater freedom but, at the same time, been faced with unprecedented troubles in security, privacy protection. In the case of introduction of electronic government in Japan (Figure 1), protection of privacy is too much stressed ideologically and efficiency, fairness and correctness of various governmental services such as national pension is not seriously recognized, which seems to be unhappy to peoples. In this way, the development of the computer and the network expands freedom of the activity of people, but simultaneously causes a serious problem such as invasion of security and privacy. Because these are mutually contradicting confrontations, there is a value conflict situation difficult to resolve. If only the expansion of freedom is pursued, it is obvious that security level declines, and individual information and privacy is seriously invaded.

We depict the three values (Expansion of Freedom, Protection of Privacy and Improvement of Security) in Figure 2.

If security is enhanced to the limit, not only freedom of activities is restricted but also privacy is infringed through intensified surveillance by cameras and E-mails.

On the contrary, if excessive attention is paid only to the protection of personal information and privacy, free distribution of information is obstructed, needless to say about a decline in convenience and efficiency, and security deterioration is induced by slow response in emergency and increasing crimes under anonymity. All these three parties are related one another with both thesis and anti-thesis, resolving the three contradicting confrontations in the state of three conflicting values of expansion of freedom, improvement of security and protection of individual information and privacy as shown in Figure 1.

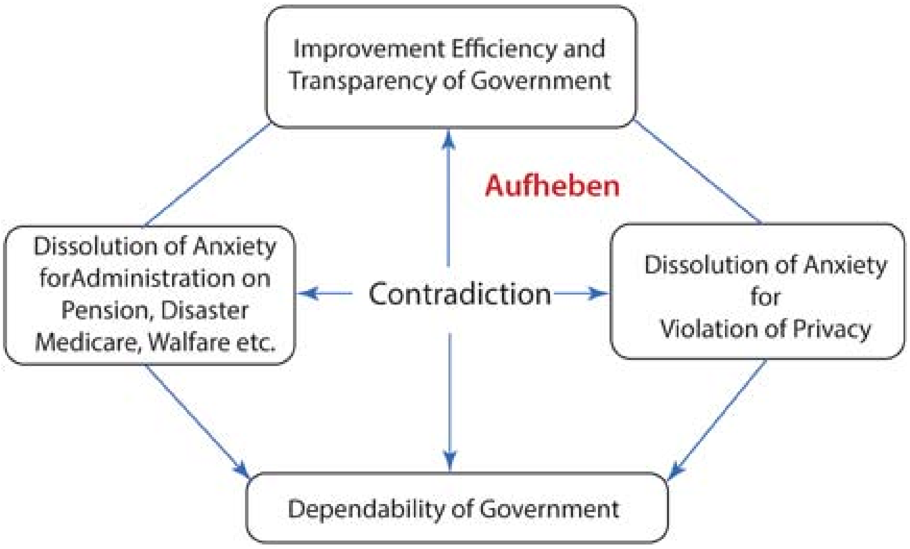

Improvement Efficiency and Transparency of Government
Aufheben
Dissolution of Anxiety forAdministration on Pension, Disaster Medicare, Walfare etc.
Contradiction
Dissolution of Anxiety for Violation of Privacy
Dependability of Government

Figure 1: Contradiction in electronic government.

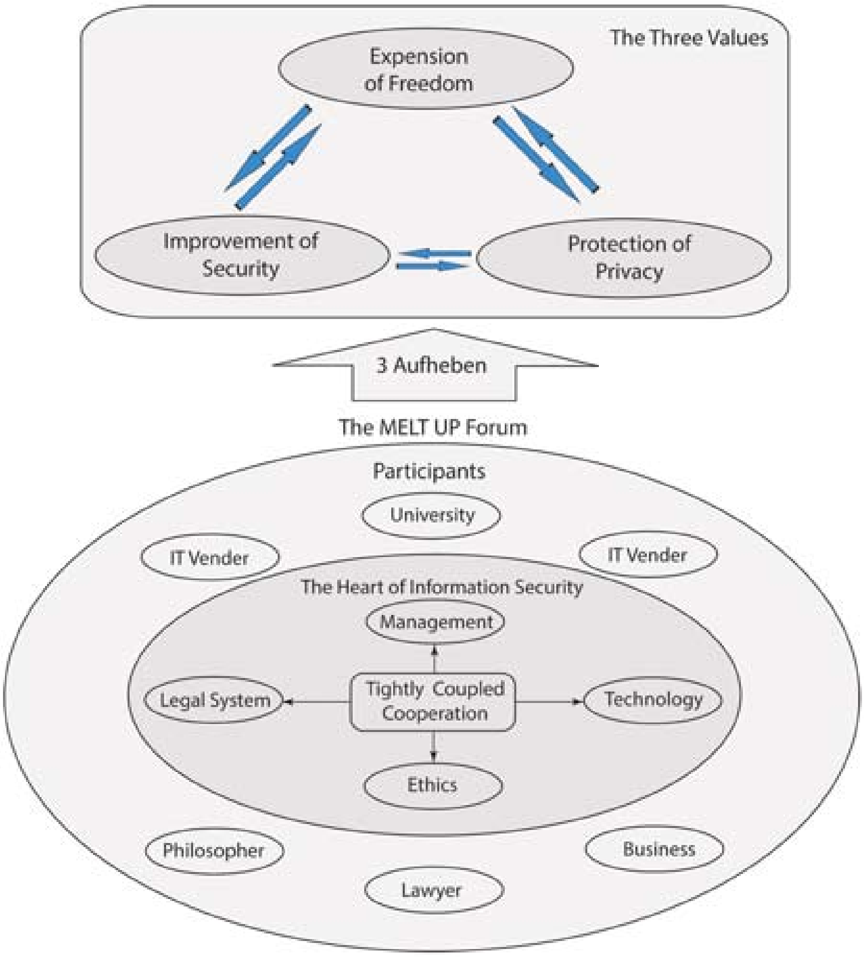


Figure 2: (sublation) of the three contradicting requirements.

Information Security of the organization requires to limit the freedom of the members, and look into their privacy. On the other hand, in many cases it often occurs that excessive protection of the privacy reduces the freedom or benefit of individuals.

We depict the relation between the three key values (Expansion of Freedom, Protection of Privacy and Improvement of Security) in Figure 2, in which the the three key values are contradict mutually. We use a German word "Aufheben," which has a meaning of "to lift up," or "to sublate." "Aufheben" unifies values contradicting each other progressively through a process of opposition and struggle and finally develop three values: Freedom, Security and Privacy for a higher stage. For achieving a meaning of "Aufheben" function, an idea of tightly coupled co-operation organization named "The MELT UP Forum" is introduced in this paper.

As shown in Figure 2, a major factors for constructing an information security is defined as The Ethics, The Law System, The Management and The Technology in which these four major factors are coupled tightly and deals with a comprehensive science across a broad spectrum of human, technological and economic endeavors. A spectrum that covers the traditional disciplines of communications, computer sciences, engineering, economics, management, manufacturing, mathematics, statistics and physical social sciences. Therefore, the information security will formalize some comprehensive science.

The MELT UP Forum is participated across a wide range of society, such as philosopher, lawyer, psychologist, physician, business manager, technologist. They argue, struggle and seek how to overcome the contradictions, irreconcilable difference among the three key values.

Tsujii has implemented the concept of promoting the information security and cryptosystem with the cooperation among Management(M), Ethics(E), Law(L), and Technology(T). So he launched the 'MELT-up' forum, meaning the improvement of the society achieved by the integrating the four fields. This forum holds seminars about the periodically. Here is an example of the MELT-up seminar:

(1) Theme: The issue of processing Japanese language in the days of Big Data Machine translation of Japanese is an important issue, since we will host the Olympic game in 2020. Besides, when a US subsidiary of a Japanese company was involved in a lawsuit, most of the cost of the pretrial was spent on translation of the internal document written in Japanese.

The current situation of Japanese language would be similar to the one of English in the late 17th century. In those days the Royal Academy took leadership in revolutionizing the language, identifying the fatal flaw that it had only emotional or sentimental expressions. English was not fitted for expressing the precise logic. They thought that England would not be able to compete with the developed countries in the Continent. That is why the English language that we know is entirely different from the Shakespeare English.

Japanese itself also has experienced the change several times, including the one during the time when the society has transformed from the aristocracy to the samurai government. Besides, Japanese was also changed in the era of Meiji, when a number of European documents were translated into Japanese. Currently Dr. Nagao, the director of the National Diet Library has been leading the advanced research and development of machine translation. The situation is changing, with the advance of the processors, so that the result of the development may be realized in the society.

This MELT-up forum was held with Dr. Takuya Katayama, the former dean of JAIST as the coordinator. We had some lectures by leading scientists in the machine translation or linguistics, and panel discussions among people in various fields.

(2) Theme: Rise, fall, and rebirth of the Japanese Information Industry Lectures about the case study of the sales activity in Latin America to promote the Television system in Japanese standard, or the analysis of the structural change in the semiconductor industry. There were also the panel discussion on the problems of Japanese society in promoting the information industry.

The relation between various contradiction and comprehensive science for information security is shown in Figure 3.

Generally implementation of the information security requires not only the technical knowledge but also the business, law, or politics. The ultimate basics would be the ethics, -discussing what is right and what is wrong. It would require the discussion based on the humanities, philosophy, etc. Therefore the information security is a comprehensive science.

My Definition of Information Security Dynamic process for establishing an integrated system of so-

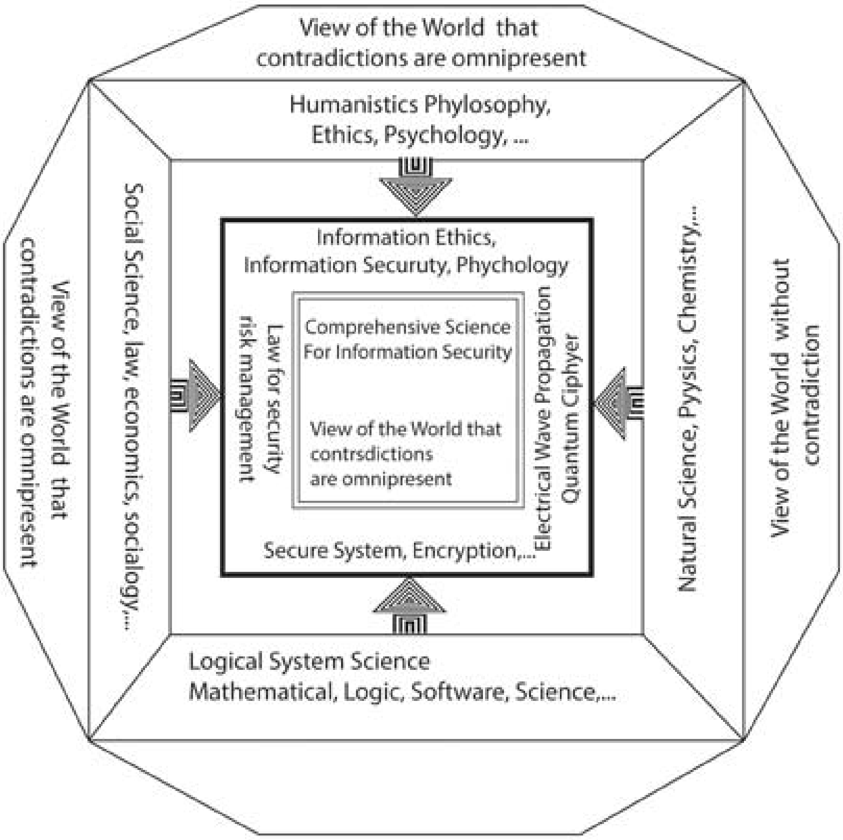

View of the World that contradictions are omnipresent
Humanistics Phylosophy, Ethics, Psychology, ...
View of the World that contradictions are omnipresent
Social Science, law, economics, socialogy,...
Information Ethics, Information Securuty, Phychology
Law for security risk management
Comprehensive Science For Information Security
View of the World that contrsdictions are omnipresent
Electrical Wave Propagation Quantum Ciphyer
Secure System, Encryption,...
Natural Science, Pyysics, Chemistry,...
View of the World without contradiction
Logical System Science Mathematical, Logic, Software, Science,...

Figure 3: Information security as the inter-disciplinary comprehensive science.

cial infrastructure de-signed to construct without infringing freedom broadened by ICT and with closer linkage and coordination among technologies, administration and management, legal and social systems, and information ethics in order to make compatible improved usability, efficiency and enhanced security, protected privacy and minimized surveil-lance over people, as shown in Figure 4.

The important thing is to train people to have the comprehensive ability. As shown in Figure 4, training in various disciplines should be given. None of them would have direct impact on the ability of managing information security. However, interaction of these disciplines would gradually raise the overall competence of the person.

1.3 Advanced Communication

Considering the above requirements in the ICT, the communication among organizations would require a new characteristic of the information security.

Traditionally the requirement of the information security is described as maintaining “Confidentiality, Integrity, and Availability.” The “integrity” is identified as “the information asset does not suffer unauthorized change.” In concrete, integrity breach is regarded as unauthorized change by the intruders or malicious program, etc. We would supplement “logical consistency” to the meaning of the Integrity. It should be confirmed whether the rule or logic included in the document contradicts to the overriding rule.

2 Organizational Cryptosystem

Cryptosystem is usually used as a countermeasure against eavesdropping. Although it is sometimes used in managing access permission, in this case it is usually linked to the user identity. Traditionally access control has been the major part of the information security and therefore most of the security efforts have been on the authentication and network security. However, as the progress of the cloud computing, protection of the information asset against the “malicious system administrators,” or storing data encrypted.

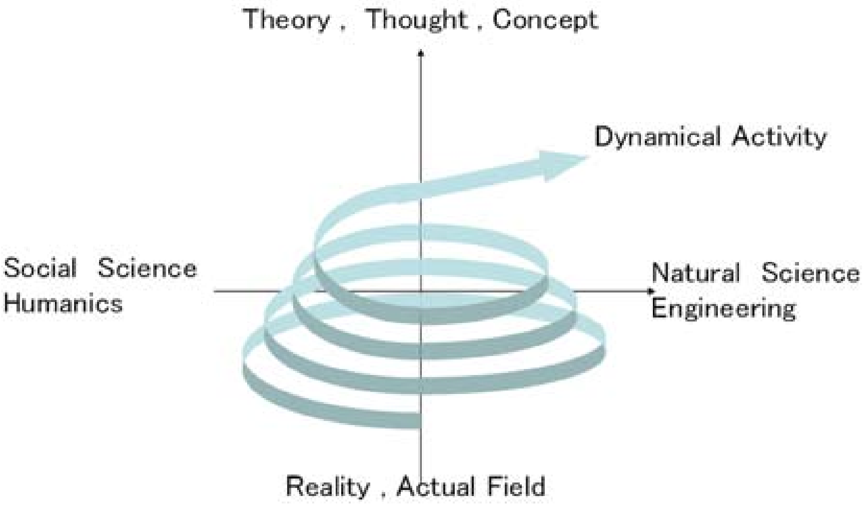


Figure 4: Educating the personnel with comprehensive ability.

If all documents are important and delicate, they should be protected also from irrelevant members in the organization. Surest way is protecting the document with cryptosystem. But usually if each document is initially encrypted, it should be decrypted in changing the assignment of the key, or access permission. It is the organization cryptosystem which enables to do it without decryption.

2.1 Inter-organizational Communication between two Companies Working on the Same Project

Figure 5 shows an example of the communication between two organizations. The sender has 3 kinds of documents, the report to the manager, a draft agreement, and a proposal of the promotion plan. The three are integrated into one document package and sent to the receiver organization.

Each of the components and the package itself has a label (metadata) describing what the document is about. They are about an important project PJ13A21, but the organizational structure or the assignment of the roles in the project is not only transparent to outside, even to the partner of the project. In such a case whole package is sent to the director of the receiver. Then the director judges who should be responsible for the activity related to the document. If the label says that the document is about the report to the manager, it should be forwarded to the project manager. If the document is about the agreement, legal person should be in charge. If it is about the proposal of the promotion, it should be sent to the sales representative.

We cannot discuss its security/reliability in the same way as the primitive electronic communications such as telephone. There is the feature of logicality/compliance, which varies according to the kind of the communication. The kinds of communication/broadcasting would be classified in a 2x2 matrix depicted in the Figure 6 [7].

There used to be only two categories until the late 20th century, the personal communication and broadcasting. However, since the beginning of the 21st century, Social Network Services (SNS) have come out. Not only do these services supply informal communication and information sharing among friends, they support exchanging niche knowledge such as the know-hows to cope with the difficulty of disability among the victims of drug-induced sufferings like the ones of thalidomide, as reported by the Firefly Research & Evaluation Limited (http://www.fiftyyearfight.org/images/Health_Grant_Evaluation_Year_3_Final_Report_July_2013_.pdf). Generally, these informal communications would require quick response or first-hand knowledge, rather than high reliability or logical consistency, which is required on broadcasting.

Then we would notice the third kind of communication, -organizational communication, which was pointed out by Tsujii [7]. The organizational communication is the ones between organizations such as companies, administrative organizations, or medical services, etc.

For that kind of system, we propose two secu-

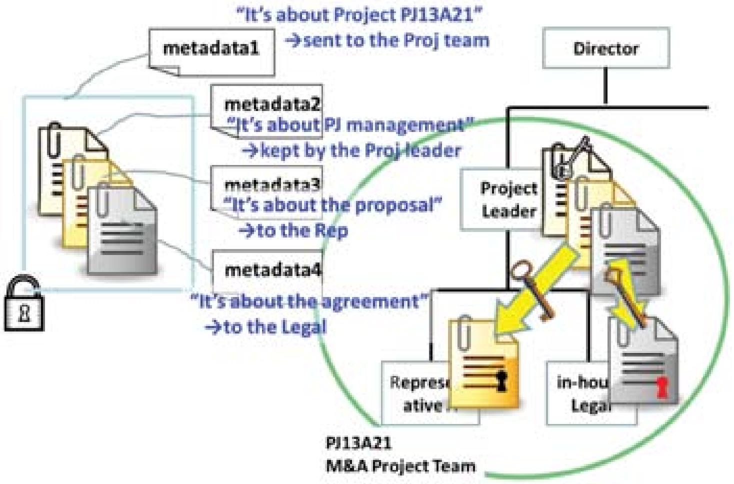


Figure 5: An example of inter-organizational communication and distribution of the document within the organization.

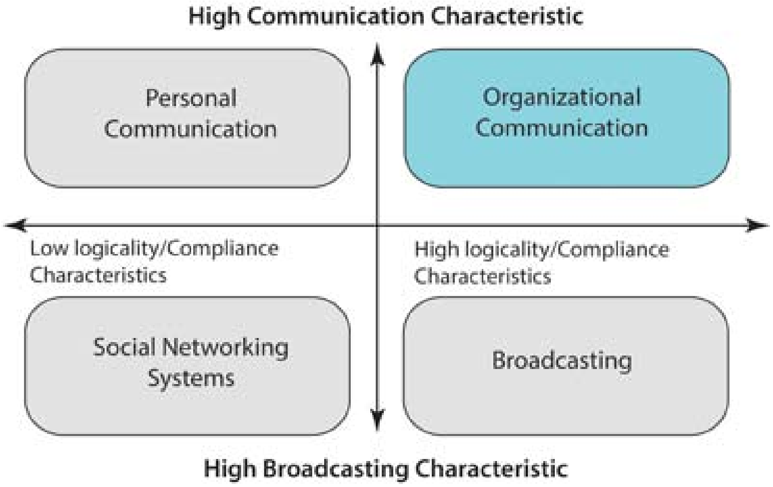

High Communication Characteristic
Personal Communication
Organizational Communication
Low logicality/Compliance Characteristics
High logicality/Compliance Characteristics
Social Networking Systems
Broadcasting
High Broadcasting Characteristic

Figure 6: Four categories of broadcasting and communication.

rity systems: One is the organization cryptosystem, which defines the access permission to the message which was sent from other organizations. This corresponds to the "Secure Inter-organizational Communication."

Cryptosystem is usually used as a countermeasure against eavesdropping. Although it is sometimes used in managing access permission, in this case it is usually linked to the user identity. Traditionally access control has been the major part of the information security and therefore most of the security efforts have been on the authentication and network security. However, as the progress of the cloud computing, protection of the information asset against the "malicious system administrators," or storing data encrypted.

If all documents are important and delicate, they should be protected also from irrelevant members in the organization. Surest way is protecting the document with cryptosystem. But usually if each document is initially encrypted, it should be decrypted in changing the assignment of the key, or access permission. It is the organization cryptosystem which enables to do it without decryption.

Figure 7 illustrates how the access permission is applied to each person. It is done by making the ciphertext decryptable with the member's secret key. It can be achieved with elliptic curve cryptosystem.

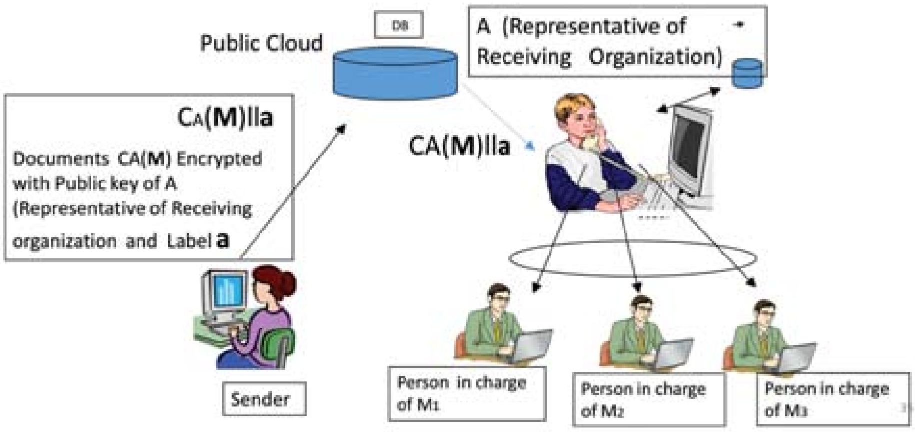

Public Cloud
DB
A (Representative of Receiving Organization)
CA(M)lla
Documents CA(M) Encrypted with Public key of A (Representative of Receiving organization and Label a
CA(M)lla
Sender
Person in charge of M1
Person in charge of M2
Person in charge of M3

Figure 7: Assigning the access permission with Cryptosystem.

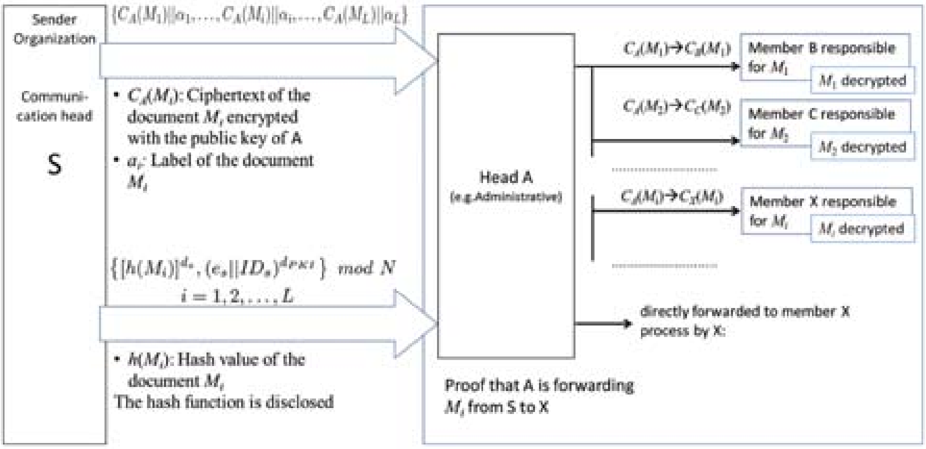

Sender Organization
Communi-cation head
S
$\{C_A(M_1)||a_1,\ldots,C_A(M_i)||a_i,\ldots,C_A(M_L)||a_L\}$
• $C_A(M_i)$: Ciphertext of the document M_i encrypted with the public key of A
• a_i: Label of the document M_i
$\{[h(M_i)]^{d_s},(e_s||ID_s)^{d_{PKI}}\}$ mod N $i=1,2,\ldots,L$
• $h(M_i)$: Hash value of the document M_i
The hash function is disclosed
Head A
(e.g.Administrative)
$C_A(M_1)\to C_B(M_1)$
Member B responsible for M_1
M_1 decrypted
$C_A(M_2)\to C_C(M_2)$
Member C responsible for M_2
M_2 decrypted
$C_A(M_i)\to C_X(M_i)$
Member X responsible for M_i
M_i decrypted
directly forwarded to member X process by X:
Proof that A is forwarding M_i from S to X

Figure 8: Practice of organizational cryptosystem.

3 Logic Cryptosystem

We introduce a private verification scheme with logic cryptosystem that it preserves user's privacy without revealing any privacy related information not only against the logic verification scheme, but also against possible malicious administrators in the World Wide Web. Basic idea of logic cryptosystem is depicted in the Figure 9. The input to logic cryptosystem to be verified by logical verification algorithm is called problems such as computer program, logical document, and Mathematics. These problems are consisted of two parts, i.e. logic part and part on privacy related values. Part on privacy related values contain some sensitive information. Basic idea of our proposal is based on separate a privacy preserving algorithm and a logical verification algorithm. In Figure 9, privacy related values are qualified to some symbols or randomized data which we call "Encryption algorithm". Cipher text is consisted of formalized part and qualified values. Formalization is processed by user himself or logic cryptosystem. Logical verification algorithm verifies the cipher text sent from encryption algorithm and generates a result, while logical verification algorithm can obtain any information on privacy related values, due to the fact that its values are qualified in encryption step. In decryption algorithm, privacy related values reserved in qualification step are used to reconstruct privacy related values. We call this step as "Decryption".

3.1 Formalization and Qualification Scheme

We depict formalization and qualification scheme in Figure 10. A formalization procedure depicted in Figure 10 relies on an syllogism. A private in-

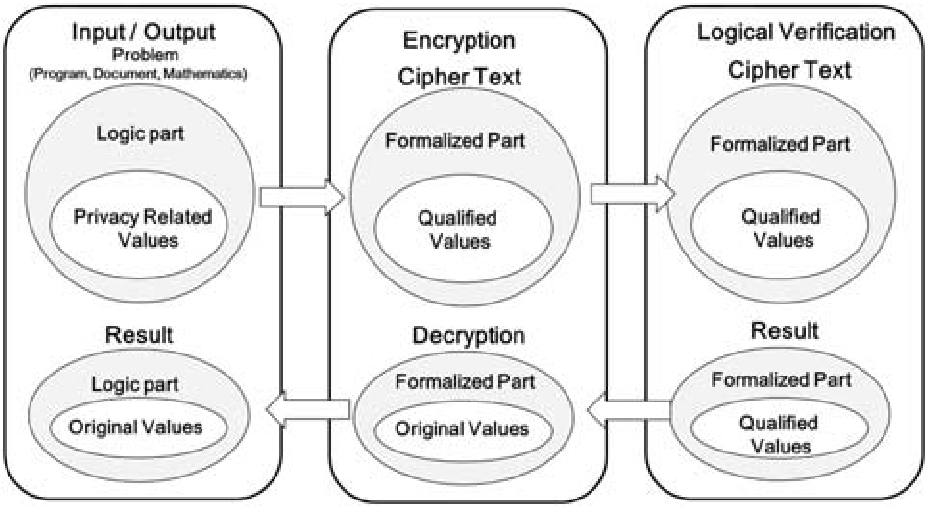


Figure 9: Basic Idea of logic cryptosystem.

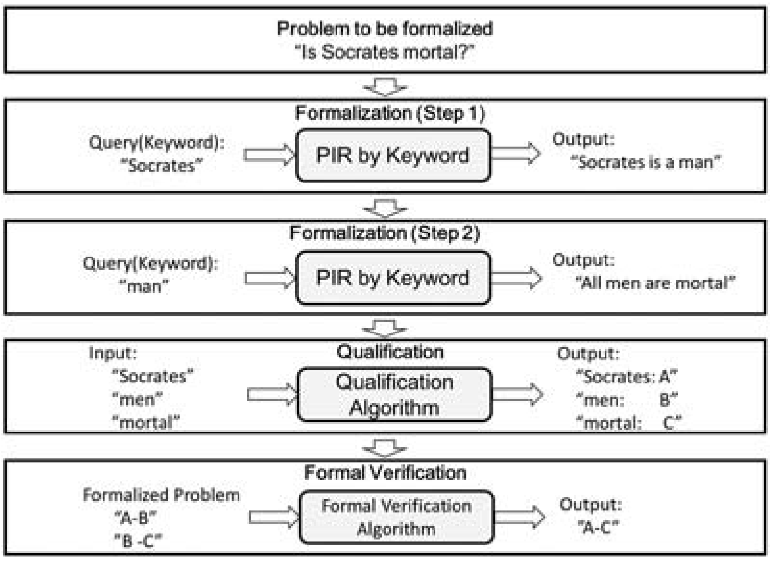

Problem to be formalized
"Is Socrates mortal?"
Formalization (Step 1)
Query(Keyword): "Socrates"
PIR by Keyword
Output: "Socrates is a man"
Formalization (Step 2)
Query(Keyword): "man"
PIR by Keyword
Output: "All men are mortal"
Qualification
Input: "Socrates" "men" "mortal"
Qualification Algorithm
Output: "Socrates: A" "men: B" "mortal: C"
Formal Verification
Formalized Problem "A-B" "B -C"
Formal Verification Algorithm
Output: "A-C"

Figure 10: Formalization, qualification scheme.

formation retrieval (PIR) protocol allows a user to retrieve an item from a server in possession of a database without revealing which item is retrieved. In this example, user selects the keyword "Socrates" from a problem "Is Socrates mortal?" makes query to PIR scheme and obtains proposition sentence "Socrates is a man" as a reply. And then he selects "man" as predicate in this sentence, and obtains reply "All men are mortal". In these steps, he retrieve replies without revealing which keyword are retrieved. Therefore privacy on two keywords are guarded. In next step, he asks qualification algorithm and obtains the symbolized data. The logical verification algorithm check its logical formulation, but obtains any information on problem expressed in natural language.

3.2 Work Flow of Logic Cryptosystem

In this section, we describe the work flow of the logic cryptosystem. Three algorithms are applied to our approaches; the encryption algorithm, Logic operation, and decryption algorithm. Work flow is depicted in the Figure 11.

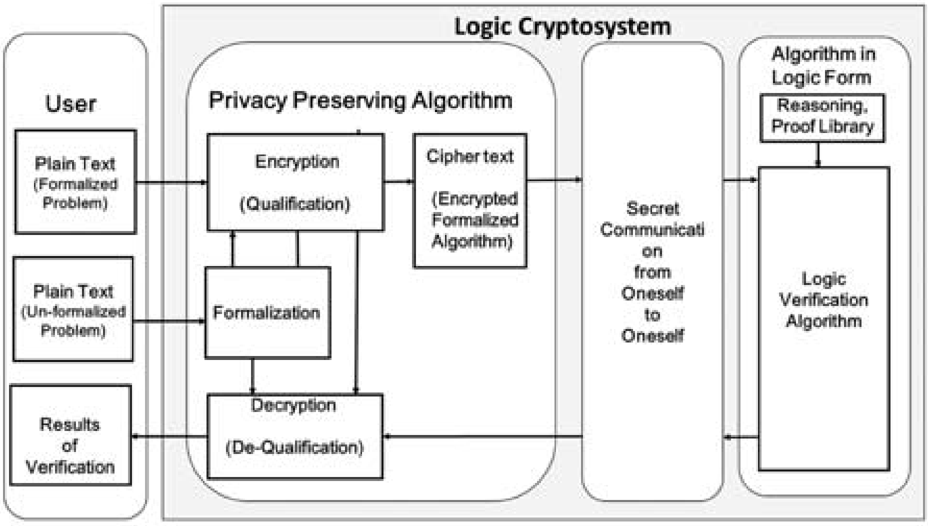
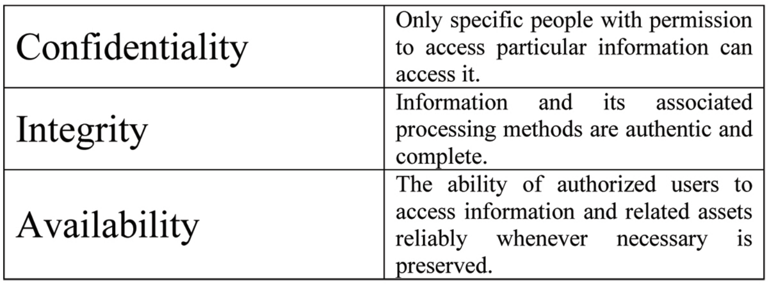

Logic Cryptosystem
User
Plain Text (Formalized Problem)
Plain Text (Un-formalized Problem)
Results of Verification
Privacy Preserving Algorithm
Encryption (Qualification)
Formalization
Decryption (De-Qualification)
Cipher text (Encrypted Formalized Algorithm)
Secret Communication from Oneself to Oneself
Algorithm in Logic Form
Reasoning, Proof Library
Logic Verification Algorithm

Figure 11: Work flow of logic cryptosystem.

Table 1: Three components of Information Security.



Confidentiality	Only specific people with permission to access particular information can access it.
Integrity	Information and its associated processing methods are authentic and complete.
Availability	The ability of authorized users to access information and related assets reliably whenever necessary is preserved.

4 Advanced Communication

Three components of information security (Confidentiality, Integrity, and Availability) were defined since 1970s depicted in the Table 1. However, due to the vast amount of communication data, and complexity of contents communicated have been arising a new demand for enhancing the quality of communication data. For example, the evaluation function of logical consistency may be helpful and effective for sender who can evaluate his sending data prior to sending to destination. We propose a new concept of advanced communication, in which logical evaluation service is able for enhancing the quality of data. We propose to apply the logic cryptosystem explained in this paper and communicate between organizations by the organizational cryptosystem.

In Figure 12, suppose some person in organization-A would like to be checked his document whether it conforms a rule of organization-B. In this case, logic checking service provider who is using the logical cryptosystem makes the communication more effective compared to current communication.

New Advanced Communication Scheme in which, users are able to enhance the integrity of the content to be communicate. The logic cryptosystem can evaluates the logicality, contradiction and consistency of the sentences, in which various legal contents such as regulation rule in the organization are included.

Therefore we would propose a system to maintain the logical consistency of the document/content depicted in Figure 13. The sender asks the Logical Verification Scheme whether the document which they are going to send conforms to the internal rule or other regulation. If the check is OK, the message is sent through the secure path to the receiver. The receiver can also check whether the document contradicts any rule.

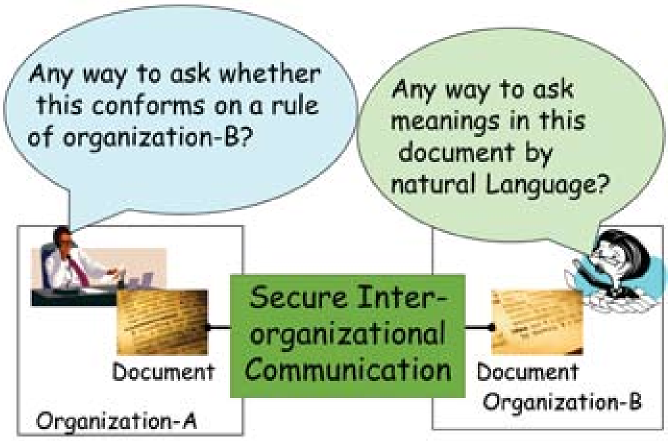

Any way to ask whether this conforms on a rule of organization-B?
Any way to ask meanings in this document by natural Language?
Secure Inter-organizational Communication
Document
Organization-A
Document
Organization-B

Figure 12: Problem in sending documents between organizations.

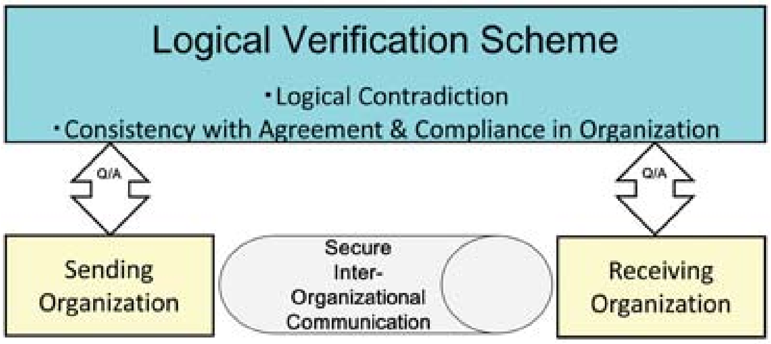

Logical Verification Scheme
•Logical Contradiction
•Consistency with Agreement & Compliance in Organization
Q/A
Q/A
Sending Organization
Secure Inter-Organizational Communication
Receiving Organization

Figure 13: Security system maintaining the logical consistency.

5 Summary

In this paper, we present an advanced concept of information security in terms of comprehensive science. Freedom, Security and Privacy are the three key values of information society. These three values are liable to conflict with each other and among them, sometimes three contradictions arises. S. Tsujii introduced a new concept of information security in terms of comprehensive science in 1993. Moreover, we have been struggling to evaluate the effectiveness of his concept by establishing a new forum named “the MELT UP Forum.” The MELT UP Forum aims to fosters, to identify and to extend a core or comprehensive science that deals with Management, Ethics, Law, and Technology across a wide spectrum of endeavors. We introduced some example of activity by the MELT UP Forum which are practically resolving the contradiction conflicting current information society. Moreover, we introduced the abstract on the organizational cryptosystem and concept of logic cryptosystem which will become the infrastructure for constructing the information security system. Finally, we also introduced the idea of an advanced communication which will aid to overcome the contradiction near future.

Acknowledgment

This study is supported by the Project entitled “Development of Public-key Cryptosystem for confidential communication among Organizations (17201)” of the National Institute of Information and Communications Technology (NICT), an independent administrative corporation of Japanese Government.

References

[1] Sheu, P.C.Y., Ramamoorthy, C.V., 2009. Problems, solutions, and semantic computing. International Journal of Semantic Computing. 3, pp. 383-394.

[2] Tsujii, S., Yamaguchi, H., Fujita, R., Okazaki, H., Shidama, P.C.-Y. Sheu, 2014. Pro-posal for logic cryptograph. 3B3-1, Symposium of Cryptosystems and Infor-mation Security 2014.

[3] H.Okazaki, K.Arai, and Y.Shidama, 2011. Formal Verication of DES Using the Mizar Proof Checker. in Proc. FCS'11, pp. 6368.

[4] H. Okazaki,Y. Aokiy and Y. Shidama, 2012. Formalization and Verification of Number Theoretic Algorithms Using the Mizar Proof Checker. Int'l Conf. Foundations of Computer Science — FCS'12 —.

[5] S. Tsujii, H. Yamaguchi, T. Morizumi, and J. Chao, 2013. Proposal on concept of en-cryption based on logic –Toward realization of confidentiality preserving of an-swer by natural language. Symposium of Cryptosystems and Information Security Kyoto, pp. 22-25.

[6] S. Tsujii, H. Yamaguchi, H. Okazaki, and Y. Shidama, 2014. Direct conversion of plain text to cipher text using logic in Q and A system. Symposium of Cryptosystems and Information Security, Jan 21-24, Kagoshima.

[7] S. Tsujii, 2014. Advance concept of information security in 4 categories – for Devel-opment of Inter-Organizational Communications. Symposium of Cryptosystems and Information Security, Jan 21-24, 2014, Kagoshima.

About the Authors

Dr. Shigeo Tsujii, Professor, Research & Development Initiative Chuo University, Tokyo, and Japan Emeritus Professor of Tokyo Institute of Technology. He graduated from Tokyo Institute of Technology in 1958. After working in NEC Corporation, he entered into the field of academics. After working in University of Yamanashi as an assistant professor, Tokyo Institute of Technology as a professor, and Chuo University as a professor, he had been the president of Institute of Information Security since April, 2004 to March, 2009. His responsibilities include: Board Chairperson of the Foundation for MultiMedia Communications (FMMC) (1998-Now), Board Chairperson of the Secure Broadcasting Authorization and Research Center (2013-Now), Board of Chairperson of the Institute of Electronics, Information, and Communication (1996-1997), and Member of the Science Council of Japan, Member of the Japan P. E. N. Club.

He has been awarded for outstanding Achievement by the Institute of Electronics, Information, and Communication Engineers, Contribution for the Broadcasting Culture by NHK

Dr. Hiroshi Yamaguchi received his B.S. degree in Instrumentation Engineering from Keio University and the Dr. Eng. degree in information Security from Chuo University in Japan. He originally joined NEC Corporation in 1963, in the Computer Software Development Department and has served as the vice president in NEC Soft. LTD. He was a Director of the basic operating systems of a super computer, large scale computer and personal computer. He also pioneered the Information Security Research Institute and the collaboration with the Universities in the USA. He worked as a head of the research and development team on the next generation electronic voting system funded by the Ministry of Economy, Trade and Industry (METI) in Japan. He was serving as a Visiting Professor in the Bioinformatics Research Institute, Waseda University, Japan since 2004. Currently he is serving as a Full Professor in the Research and Development Initiative, Chuo University, Japan. He served as a President of Software Engineering Society (The SES), and currently serving the research fellow of the Society of Development and Process Science (The SDPS) and a Vice President of Academy of TransdisciplinaryLearning & Study Studies (The ATLAS). He is currently engaged in the research project funded by the National Institute of Information and Communication Technology (NICT). He is currently working as a subdirector of the Melt-up Forum participated from Japanese Government, major IT venders in Japan. His research interests focus upon the cryptographic theory, modern logic cryptology and cognitive science. He received the best paper award on information sharing on DOD 14th ICCRTS, 2009. He has been a keynote at several international conferences, such as IEEE-ICTAI, HASE, IEEE-BIBE, SDPS, and

IEEE-ISM.

Dr. Masahito Gotaishi, Associate Professor, Research & Development Initiative of Chuo University, Tokyo, Japan. He graduated from the faculty of Agricultural Chemistry, University of Tokyo. After working in Meiji Milk Product, he earned the degree of MBA in Warwick Business School. He experienced businesses of manufacturing, consulting, and software industry. While working in the business field, he was responsible for introducing overseas security software into the Japanese market. After that, he entered into the field of education. His field includes Hands-on Unix Security training course and Security Management course. Currently he works in the Research & Development Initiative of Chuo University to continue the study of post-quantum cryptosystem. He is also working as a lecturer of Calculus and Linear Algebra for the students of a general education course.