日本財団 The Nippon Foundation 助成

IIPS

Institute for
International Policy Studies
・Tokyo・

IIPS International Conference

"The IT Revolution and Security Challenges"

Tokyo

December 10-11, 2002

"Information Security
−Driving Force behind the IT Revolution"

by
Shigeo Tsujii
Professor
Faculty of Science and Engineering
Chuo University
Japan

Institute for International Policy Studies

Symposium

- The IT Revolution and Security Challenges -

Information Security –Driving Force behind the IT Revolution

10 December 2002

Chuo University Faculty of Science and Engineering
Information and Systems Engineering Department

Shigeo Tsujii

1. Preface – A Change of Perspective

Hegel (1770–1831)

“History… is none other than the progress of the consciousness of freedom, and we must recognize its inevitability.”

Contemporary researcher in cryptography (1933-?)

“What a genius Dr Hegel was! His admirable vision transcended the time and place in which he lived. At the dawn of the 21st century it seems as if the computer, like God, is omnipresent, and that its continuing ubiquity will bring marked increases in our freedom. However, hand-in-hand with the growth of freedom, various inherent anxieties and insecurities are manifesting themselves. As a contemporary cryptography researcher, I think about ways to use encryption technology to enhance freedom, while reducing to a minimum any issues of security, or concerns relating to the possible creation of a surveillance society. Today I would like to address these matters, with reference to various examples such as electronic voting systems.”

It could be thought that Hegel's principle, that history is the process of the development of freedom, which was framed in reference to the real world, is even more applicable to the real world when it is combined with the added dimension of the cyber-world.

For example, encryption technology—a core technology in the field of information security—is thought of solely as a technology for protecting the cyber-world, whereas in reality it is expanding the cyber-world and bringing people greater levels of freedom. Let us consider these matters in relation to electronic voting and electronic surveys.

At present, Japanese local governments are attempting to introduce voting systems for voters at polling stations. In a genuine electronic voting system, the voter can vote from any terminal and from anywhere via the Internet or a similar medium.

If this type of genuine electronic voting (henceforth referred to simply as “electronic voting”) becomes possible, it is predicted that the percentage of people voting will rise, bringing significant change to the current political landscape, in which voting rates have been declining.

Electronic voting need not be confined to elections only; it will also become easy to issue questionnaires and conduct surveys on individual political issues, thereby significantly increasing freedom of political involvement citizens. With electronic voting, anonymity must be guaranteed; in e-business and related fields too, many people would be willing to reply to questionnaires, provided that they could do so anonymously. The construction of such a system would enable businesses to operate successfully using the "information pull" model.

In addition to the necessity for preserving voter anonymity and protecting against voting irregularities (such as the casting of multiple ballots), electronic voting (or any comparable activity) imposes the following strict requirements which must be satisfied in a verifiable manner: that the vote-tallying center must calculate the vote totals properly, that the ballot-counting stations must count the votes properly, and that the preferences of individual voters must remain absolutely secret.

For the first time, solutions to this kind of major challenge are now generally being implemented using current encryption technology, such as public-key encryption and zero-knowledge interactive proofs.

For this reason, information security technology—including encryption—is not merely a technology for the purposes of protection, but a technology which also enhances the growth of individual freedom and forms a solid foundation for the new cyber-world.

However, the growth of the cyber-world is also bringing out people's anxieties about safety and their fear of an omnipotent society.

In an article entitled "A Discussion of the Freedom of Information—the Power of Data and the Ethics of Encryption," serialized in the October 2002 issue (No. 172) of the "Central Review," the philosopher Hiroki Azuma writes the following:

> **The Two Strata of Post-Modernism**
>
> Diversity of requests and thoroughness of information control—readers may well feel that these two coexisting tendencies are mutually contradictory. However, there is no contradiction here. This is because this new control which is being demonised in this case is different from that of Big Brother, as depicted by Orwell. It is not related to ideology – in short, it is not related to any sense of values or norms.
>
> Although it is good that diverse values exist, and with maximum possible recognition for civil and economic liberty notwithstanding, if information solely on who did what, when, and where, is always collected, this could if necessary

have a profound effect on the lives of certain individuals. Moreover, this information is collected without the individual's knowledge, as in the example of the automatic ticket machine cited at the end of the previous installment. This is a characteristic of the power to control the environment, which underpins post-modern society.

The stratum of diversity and the stratum of information control, the ideology stratum and the security stratum, in other words the stratum ruled by the principle of tolerance and the stratum ruled by the principle of exclusion. It is a characteristic of our society that these two strata remain separate.

We specialists in encryption and information security assume an obligation to eradicate fears of this kind of omnipotent society. At the same time, while preserving safety and reliability for individuals, companies, and vital infrastructure at every level of state and society, we assume an obligation to construct an environment in which the privacy of individuals is protected and freedom can be enjoyed. To achieve all of the above requires a finely detailed scheme to increase freedom, improve safety, and quell fears of an omnipotent society; this scheme must meet the challenge of balancing mutually contradictory requirements, introduce methods such as decentralized authority and management, and achieve compatibility between its three goals. Cooperation in every aspect—technology, management and administration, the legal system and ethics—is indispensable.

Moreover, it is desirable that all citizens of the cyber-world—not just the specialists in the fields mentioned above—should be more conscious of the need for information security.

A full 10 years after first establishing information security guidelines in 1992, the Organization for Economic Cooperation and Development (OECD) released revised guidelines in August 2002. Whereas the old edition set out ideas for measures to protect the safety of computer systems, the new edition, entitled *OECD Guidelines for the Security of Information Systems and Networks*, propounds the necessity for strong safety measures in response to the diverse threats currently posed in the global network environment with its open information systems. These ideas are expressed in nine principles. Within these principles, the two expressions “culture of security” and “participant” stand out. There are as many definitions of “culture” as there are cultural anthropologists; however, the author of this paper would define culture as the sum total of a given group's inherent values, ethics, behavior patterns, and lifestyles. If culture is interpreted in this way, then the participants on the network comprise a

group (that is, the entire population of the cyber-world, not just the information security specialists), and it can be said that the new guidelines make an appeal to all the people of the advanced IT nations to share in an awareness of information security.

In our capacity as specialists we must design systems that meet with society's approval and also accept the responsibility for explaining matters to society at large.

2. The Ubiquitous Society and Increases in Freedom

Computerization is progressing in different spheres of society. Not a day goes by without a flood of newsprint devoted to e-money, computerized medical records, electronic voting, computerized tax filing, e-government (both national and local) or some other computerized activity.

Let us call this society, in which computerization is advancing on many fronts, the "ubiquitous society." The ubiquitous society may be regarded as a society based on a foundation of computer and information network technology. Within that complex multi-dimensional space, one can make use of various coordinate axes. However, to the author of this paper, there are many social issues to consider relative to the coordinate axes of freedom and safety.

The question "What is freedom?" is a difficult one to answer. However, with the advent of networking founded on digital technology, various barriers between organizations have been lowered and society has assumed a contiguous structure. If one looks at the effect of this on freedom of behavior, it cannot be denied that the various practical benefits brought about by computerization have also resulted in increased personal freedom. Let us explain this in slightly more detail.

The digital technology underlying the spread of ubiquitous computing is creating a borderless world through the power of distributed computing. More fundamentally, it is connecting all corners of society. Looking at the larger picture, as this technology brings about a continuous structure in society, it is also giving rise to a paradoxical phenomenon, which can only be described as a "digital analog" identity crisis.

In the same way that all matter is formed of atoms and molecules, all forms of information, such as sounds and images, can be digitised into signals representing 0 or 1. As the ubiquitous computer, linked by network to its peers, has become a staple of society, it is now easy to process, edit, generate, transmit, search, and share this information.

This has become a major factor increasing the interconnectedness of manufacturer and consumer, author and reader, broadcasting and communications, government and people, public and private, the internal and external workings of a company, businessman and individual, workplace and home, work and leisure, politician and citizen, nation and nation, scientific and cultural pursuits, and so on and so forth, removing the time and space barriers between industries, organizations, and regions with a momentum that gives rise to a principle called the interconnectivity of society.

For example, in the realm of copyright too—the key to the increased popularity of

digital broadcasting and the like—the phenomenon of continuity between creator and consumer is progressing. For many consumers it is now easy to edit original information and add one's own ideas to it. There are many such cases in which the principle of "fair use" is substantially violated.

Thus, while the barriers between different systems and groups are being lowered and freedom is spreading, it is also true that causes of anxiety and elements of danger continue to increase in number.

In the realm of computer and network crime, a criminal act committed in cyberspace may have an immediate effect in a location on the opposite side of the world, or may even leave no trace at all, if the location in which it was committed cannot be determined.

In addition, threats to e-society are posed not only by people acting in bad faith or with malicious intent, but also by human error and breakdowns or other calamities occurring on computers and other information devices.

Given this situation, the greatest challenge of the ubiquitous society is to enhance safety so that people can enjoy freedom to the greatest extent possible. Freedom must have a safe and solid platform on which to stand. In the following section, we will consider the framework of information security.

3. Constructing the Ring of Information Security

Information security is usually defined as follows:
Information security is the protection of information assets, in terms of confidentiality, integrity, and availability, against various threats and attacks on their security, so that normal functions and conditions are preserved, information systems and the reliability of information is enhanced, and users can use information systems in peace of mind.

Hence, since the 1970s “confidentiality,” “integrity,” and “availability,” the initials of which spell “CIA,” have been regarded as the three components of information security. These concepts are formally defined in Table 1

Table 1. Confidentiality, Integrity, and Availability

Confidentiality	Only a person who has 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

To put it simply, “confidentiality” is the protection of privacy and industrial secrets. For a long time encryption has figured prominently as a means of achieving confidentiality. “Integrity” means that information cannot be falsified. If a website has been altered by someone who is not authorized to do so, its integrity has been compromised.

“Availability” signifies that a person can use a resource such as a computer whenever he wishes to. If a DoS (denial of service) attack, for example a spam attack, renders a mail system unusable, then its availability has been compromised.

Do these three elements together constitute a complete definition of information security? Although explanations like the one above appear in recent literature on the subject, if one considers the importance of electronic certification, one has to say that this is an inadequate definition.

When electronic business transactions, e-government business and the like are carried out, it is essential that it be possible to verify the identities of both the parties involved. If it proves impossible to confirm a person’s identity with absolute certainty—whether due to intentional deception or accidental error—e-society will collapse completely. The invisibility inherent in the cyber-world makes it a fertile environment, both for malicious deception and accidental error. To protect against this kind of occurrence, it must be possible to carry out electronic certification reliably using

identification of individuals and digital signatures.

In accordance with this line of thought, some recent commentators have added a fourth information security element—certification—to the existing trio of confidentiality, integrity, and availability. The concept of provability includes the notion that a transaction will leave behind a record of the time at which it took place, as proof that it took place. Some may think that the notion of certifiability is easier to understand than provability; however, the prevailing view seems to be that it is easier for people to comprehend and remember three elements than four. The author too is undecided, but my current thinking is as follows.

The definition of integrity given in Table 1 is somewhat abstract. It is also possible to frame a definition of integrity that also includes reliable certification and proof.

In short, 20 years ago integrity was understood to mean “error-free data.” However, for practical purposes it would seem preferable to expand the definition to encompass the concepts of certification and proof.

This kind of information security, then, is not something that can be protected using technology alone. Management and administration within organizations must be carried out reliably. People working in organizations must apply high ethical standards. Information ethics are important. However, since it cannot be assumed that all people are virtuous in nature, a system of laws to deal with information crime must be put in place.

Ultimately, to achieve information security these four items—technology, management and administration, the legal system, and ethics—must be interlocked with one another to construct a ring of strength, as shown in fig. 2.

Let us consider the car, which is a metaphor that is easy to understand. To enable trouble-free driving, the following are required:

(1) Technology: both the car's components, such as the engine, and the car itself (the finished product comprised by the components) must be well designed.
(2) Management and administration: even if one has purchased a car of high quality, it is important to keep it in good condition by carrying out maintenance checks diligently and sending it for periodic inspections, to improve one's driving technique, and to always drive safely.
(3) Legal system: traffic laws and a legal system to deal with violations of these laws must be properly established in advance.
(4) Ethics: it is important that everyone adheres to good driving etiquette.

This analogy makes it easier to explain how technology, management and administration, the legal system, and ethics apply to information security.

(1) Technology

In addition to encryption technology—the main theme of this paper—the list of technologies also includes technology for identification of an individual using bio-information, technology for the protection of copyright using electronic watermarks and the like, counter-measures to combat viruses, firewall technology, and network security technologies such as intrusion detection systems (IDSs). For example, it is presumed that encryption is used to conduct narcotics dealing in secret. In order to fully utilize technology for the safety of individuals and society, it is necessary to construct a watertight wheel of security that fully encompasses management and administration, the legal system, and ethics.

The phrase “information security” contains strong overtones of protection. Encryption is the core technology in information security. But is encryption only a technology for protection? In fact, encryption is a driving force behind computerization and an engine of revolutionary change in society. Let us consider e-money as an example.

e-money is a currency in which technology such as digital signature technology (based on public-key encryption) is used to attach value to information to represent an amount of money. The banknotes in use today derive their monetary value from the use of advanced printing technology and paper quality. However, in the cyber-world, which is built out of computers and networks, it is not possible to produce a currency where value is accorded based on material attributes. This currency will come into being as follows: using public-key encryption, only currency issuers, such as the Bank of Japan, will be able to use their secret private keys (which are kept secret) to perform a mathematical operation to attach a digital signature to information representing an amount of money.

e-money is in the vanguard of e-society and it is said that in the future it will bring about a seismic shift in the international economy. It is only with the advent of encryption that it has become possible to implement the e-economy system (of which e-money forms a part). This is also true of a great majority of the systems introduced as part of the computerization of society, such as e-government systems (both at the national and local levels) and computerized medical record systems. In light of this, it might be argued that to regard encryption as simply a technology of protection is to seriously belittle it.

This type of information security, which incorporates encryption technology, is much more than a framework for “protection” and can be seen as a firm foundation on which to construct society.

(2) Management and administration

How can information security be preserved in organizations such as companies and local governments?

Firstly, it is essential to clarify which of the organization's information assets need protecting, carry out analysis to determine the potential threats to these assets, and formulate a security policy. This policy will be a set of rules (like a constitution) determined at senior management level, and based on the organization's management principles. Secondly, it is necessary to adapt the international standards laid down by bodies such as the ISO (the International Organization for Standardization), or the established domestic standards based on these standards, to the business or organization, and determine practical criteria and guidelines.

In the field of information security the following international standards are well-known:

ISO/IEC 15408

ISO/IEC 17799

The IEC is the organization known as the International Electrotechnical Commission. Standards determined jointly by the ISO and IEC are written "ISO/ICE;" however, these two standards are abbreviated below as ISO 15408 and ISO 17799. A brief explanation of these two standards is in order. ISO 15408 is laid down as a provision standard for when organizations purchase so-called IT (information technology) products, such as computers or IC cards. This standard effectively started life in the mid-1980s as a computer procurement standard established by the US Department of Defense. Subsequently, starting in around 1990, extended standards were determined for general government and civilian use. This also took place in various European countries, such as Germany and the UK. These standards were combined into what is now ISO 15408. ISO 15408 consists of functional requirements and warranty requirements. Functional requirements define the required functions of an IT product. Warranty requirements define the degree of reliability to which the product's purported functions are guaranteed when the product is implemented.

Functions are divided into 11 categories as shown in Table 2. These categories are then further subdivided. There are two categories which relate to the use of encryption: encryption key management functions and administration functions required for use of encryption. In general, if advanced features are requested in IT products, it is assumed that these features will also be designed to function reliably. Hence, the US Department of Defense standard of the 1980s did not distinguish between functional

requirements and warranty requirements, but regulated the two together in terms of IT product safety levels. In about 1990 Germany developed the idea of regulating these two sets of requirements separately, and the present-day ISO 15408 standard is now structured accordingly.

In Japan it can be said that the history of ISO15408 began in 1997. This is an absolutely shocking fact. In fact, in the early stages of the 1990s, the author served as chief investigator on the Security Subcommittee to the Open Environment Consolidation Committee established by the Ministry of International Trade and Industry (as it was then known), and carried out a detailed investigation of computer security evaluation standards in the US and Europe. In Japan, however, awareness of information security was low (users particularly were indifferent to it). In addition, there exists an unspoken perception that, since the manufacture of advanced products is Japan's forte, and since manufacturers' after-sales service is also of high quality, these types of standard are unnecessary. There was also strong sentiment that the higher product costs and increases in time-to-market resulting from compliance with these standards would be serious drawbacks. In addition, the prospect of internationally recognised or global standards did not carry sufficient weight. For reasons such as these, there was little stimulus in Japan for debate regarding computer security evaluation standards, and discussion stagnated.For these reasons, Japan lags approximately 10 years behind Europe and the US in terms of human resources training in this field. This is becoming a serious problem.

ISO 15408, which was explained above, is a procurement standard for organizations buying IT products. The standard that defines management measures for the use of IT products, information systems and the like which have already been purchased, is known as ISO 17799. This ISO standard has been adapted from Part 1 of the UK standard BS 7799 (which consists of a Part 1 and a Part 2). As shown in Table 3, it is divided into 10 different management fields. In Japan the ISMS (Information Security Management System) has been established in conformity with these standards.

Table 2
ISO 15408 Security Function Categories

Security auditing
2. Communications/denial prevention
3. Use of encryption
4. Protection of user data
5. Identification and verification
6. Security management
7. Privacy
Security function protection
8. Availability and resource management
9. Access control
10. High levels of authenticity and reliability

Table 3
ISO 17799 Information Security Management Fields

1. Security policy
2. Security organization
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and application management
7. System development and maintenance
8. Access control
9. Business continuity planning
10. Compliance

(3) Legal system

In order to get society to make use of technology, it is necessary to make adjustments to the legal system. For example, the electronic signature law—or "Law Concerning Electronic Signatures and Certification Services" to give it its exact name—came into effect in April 2001. With this law, a legal foundation was established enabling people to use digital signatures that use public-key encryption to conduct e-business transactions and e-government activities (both national and local) in peace of mind.

A discussion of the legal system is beyond the scope of this document. However, several laws relating to information security which are being deliberated at the time of writing (July 2002) are shown in Table 4.

Table 4. Examples of Laws Relating to Information Security

Name of Law	Date of Enactment/ Effective Date
Draft Law on Protection of Information on Individuals	Under deliberation
Law for the Protection of Computer Processed Data Held by Administrative Organs	Under deliberation
Law to Amend Sections of the Criminal Law	2001/7/4
Draft Law on Amending Sections of Commercial Law	2001/11/28 2002/4/1
Electronic Consumer Contract and Electronic Consent Notification Law	2001/6/29
Law Concerning Electronic Signatures and Certification Services	2000/5/31 2001/4/1
Copyright Law (revised in 2000)	2000/5/8
Commercial Registration Law (revised)	2000/4/19
Notary Public Law (revised)	2000/4/19
Law on Enforcement of the Civil Code (revised)	2000/4/19
Law on Monitoring of Communications for Investigation of Crime	1999/8/18 2000/8/15
Law on Citizens Register (revised)	1999/8/18
Law Prohibiting Unauthorized Access	1999/8/13 2000/2/13

(4) Ethics

Although we speak constantly of ethics, there is an element of doubt about whether ethics can exert any influence in advancing information security. However, this is mankind's first attempt at constructing the cyber-world; and in the course of this process, the rapid rise of values and morals relating to information will, in the opinion of the author, become a great unseen force in advancing information security. I will say no more on this subject.

In conclusion, although I have discussed how it is only with strong cooperation between technology, management and administration, the legal system, and ethics that information security can advance, in this lecture I would particularly like to highlight the example of electronic voting systems. Using encryption technology to protect against dishonest activity, electronic voting systems are overcoming the major challenge of privacy protection and paving the way to e-democracy. As such, they constitute an excellent example of the points discussed above.

4. The Development of Modern Cryptography

The preceding sections have sketched out an overview of information security. Here let us summarize a topic frequently referred to already—recent trends in modern cryptography (the main subject of this document).

Although the history of cryptography goes back several thousand years, cryptography as we understand it today began no more than about four and a half centuries ago. “Modern cryptography” refers to the cryptography which performs an essential role in e-society, which is based on the technological foundation of computers and networks, and also in the ubiquitous society.

Less than 30 years after its birth, modern cryptography has now matured in technological terms, and, in a profound sense, has spread its roots widely to become a foundation of society. Even though it may be premature to try and chart the development of modern cryptography, due to various 1990s phenomena such as the systematisation of research into safety theory, the dramatic rise to prominence of the computer, and the resultant rapid growth of the Internet, one might think that, at the end of the twentieth century, the world of cryptography is also beginning anew. Accordingly, although it is somewhat crude, let us think of the final period of the twentieth century as the first era of modern cryptography, and the dawn of the twenty-first century as the second. (See fig. 7.)

In the first era shared-key encryption is represented by DES (Data Encryption Standard) and public-key encryption is represented by ordinary (or primitive) RSA.

Twenty-odd years ago DES was established in 1977 as the standard encryption method for use by the United States’ government. Now, despite its historic role, its mission is about to end, due to factors such as the limitations of the 56-bit key length and Matsui’s linear cryptanalysis proposition. In the United States AES (Advanced Encryption Standard) has been established in place of DES. In general, a key length of 128 bits is used. With regard to safety, safety certification (expressing safety certifiability) must be attached, indicating the ability to withstand well-known attack methods, such as the diff decryption method and the linear decryption method.

On the other hand, although RSA encryption has for a long time reigned supreme in the field of public-key encryption, here too significant change can be seen on two fronts. Firstly, based on both empirical and theoretical evidence, it appears possible that the basic (primitive) RSA method may not be capable of withstanding an active and adaptable decryption attack. Accordingly, around the year 2000, it was recommended that the RSA-OAEP method, which carries out pre-processing, be used as the primitive

RSA method. When exposed to any kind of powerful attack, even plain-text 1-bit information cannot be decrypted (provided that the primitive RSA method is one-way). This kind of processing is required for all public-key encryption, not just for RSA encryption.

In the field of safety theory, recently a more advanced and refined paradigm, KEM (Key Encapsulation Mechanism) has emerged. Together with El Gamal public-key encryption, which relies on the difficulty of the discrete logarithm problem, this allows a more unified and generalized description.

Another development in public-key encryption is the implementation of elliptic encryption. RSA encryption relies on the difficulty of prime factor decomposition. However, since calculation for decryption requires standard exponential time, in order to combat computer ubiquity and the exponential increase in computer processing power over the years, the number of digits in the factors used must be continually increased. At present, the key length is 1024 bits; however, within 10 years it will probably be necessary to increase the key length to 2048 bits. By way of comparison, elliptic encryption and fast elliptic encryption rely on the difficulty of the elliptic curve discrete logarithm problem. Calculation for decryption requires exponential time. The same level of safety achieved using the RSA method and a key length of 1024 bits can be guaranteed by elliptic encryption with a key length of approximately 160 bits.

In addition, compared to RSA encryption, these types of encryption require relatively small increases in key length to cope with the threats posed by increased computer processing power and computer ubiquity. For example, whereas the key length for RSA encryption will have to be increased from 1024 bits to 2048 bits, it is estimated that elliptic and fast elliptic encryption will only require an increase from 160 bits to 210 bits.

In practice, elliptic encryption, which was invented in the mid-1980s, is attracting great attention. This is due to the merits of applications such as the use of public-key encryption to verify identity by embedding the private key on an IC card—the potential passport to the cyber-world.

In addition to the various technological changes which have taken place, there have also been other advances. As mentioned previously, on the legal front the “Law Concerning Electronic Signatures and Certification Services” came into effect in April 2001. In regard to standardization, a committee (known as CRYPTREC) with members drawn from the Ministry of Public Management, Home Affairs, Posts and Telecommunications, the Ministry of Economy, Trade, and Industry, communications and broadcasting organizations, information-processing promotion associations, the

bureaucracy, universities, NTT, the world of industry and various other fields, was formed in the fiscal year 2000 to identify encryption technology which could be used in e-government. This committee continues to carry out its activities with great vigor.

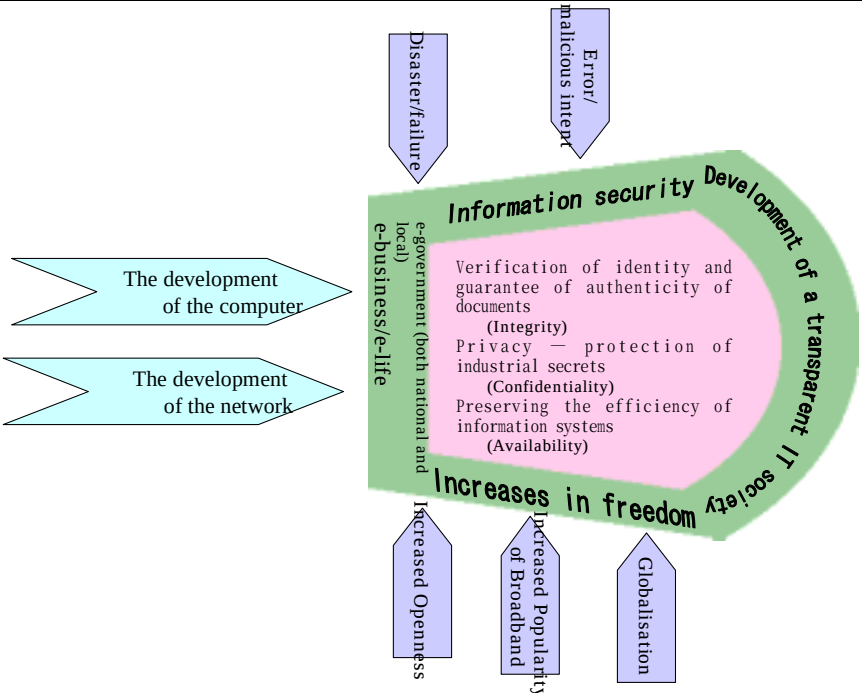

Fig. 1 Information security and the development of an IT society

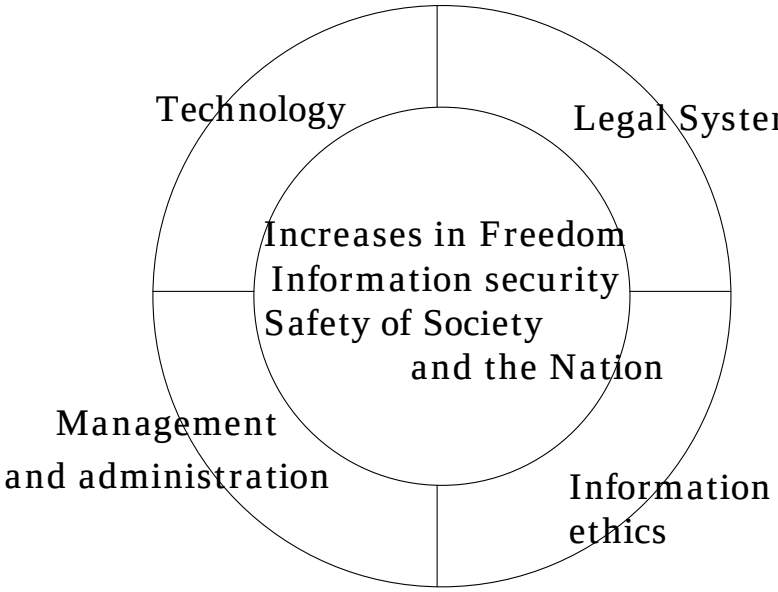

Fig. 2 Constructing the wheel of information security

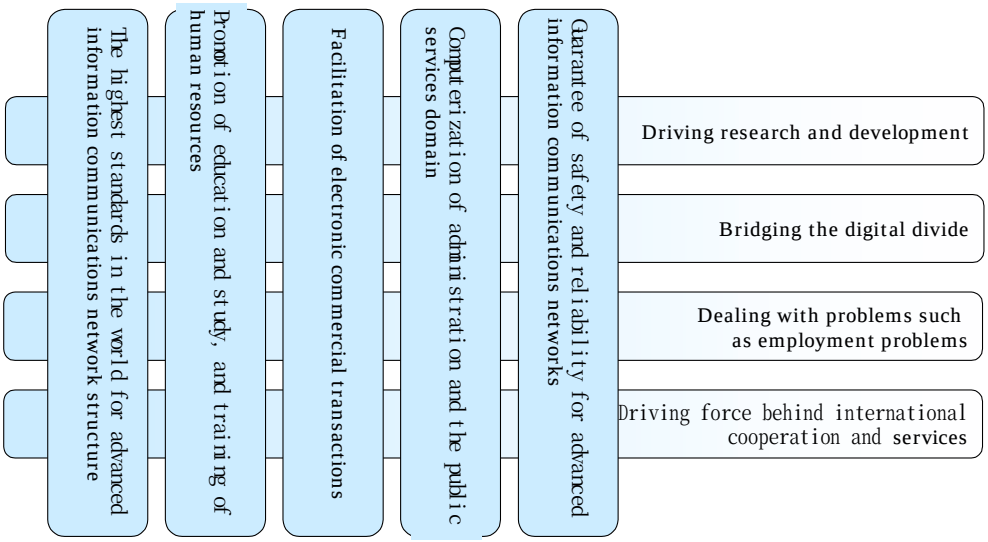

Fig. 3 IT Strategy Headquarters' e-Japan Strategy

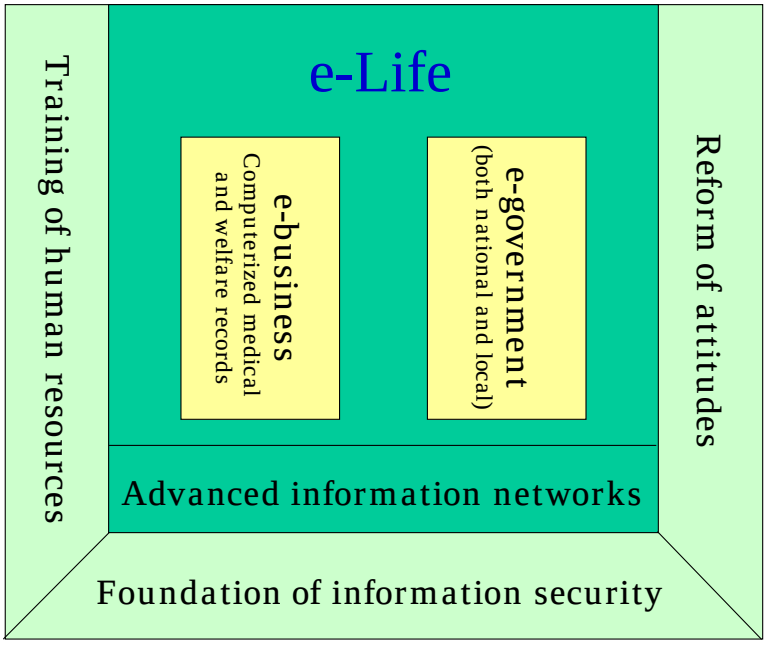

Fig. 4 e-Japan

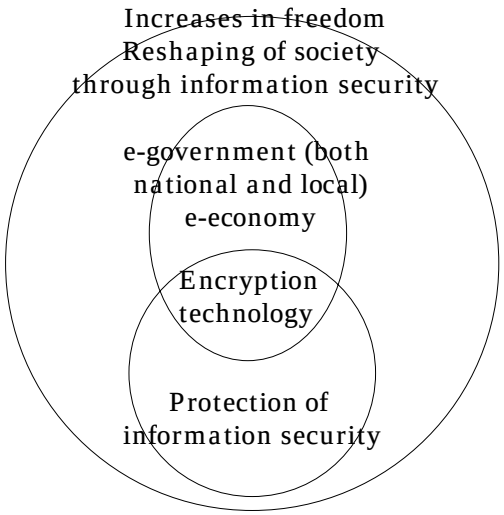

Fig. 5 Encryption and information security
—driving forces behind the e-society

Type \ Methods	Secrecy	Verification
Shared key	◎	○
Public key	○	◎

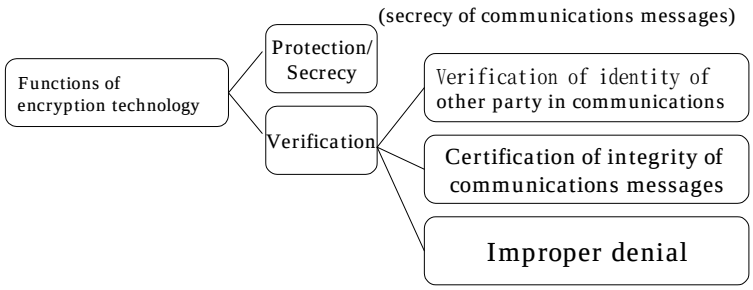

Fig. 6 Methods and functions of encryption

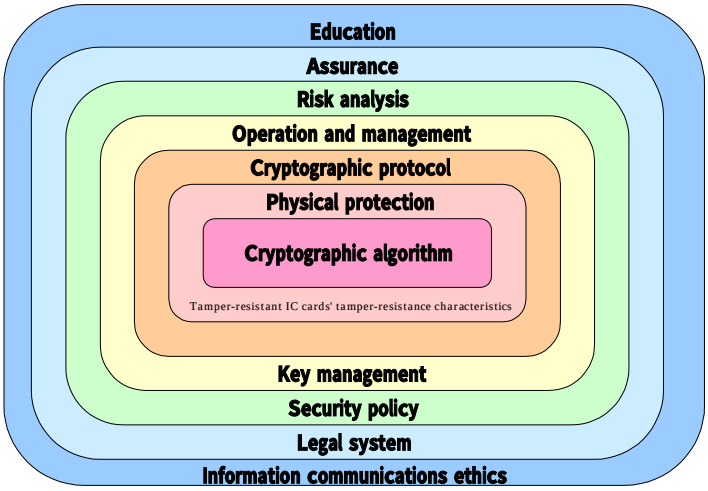

Fig. 7 Information security from the viewpoint of cryptography

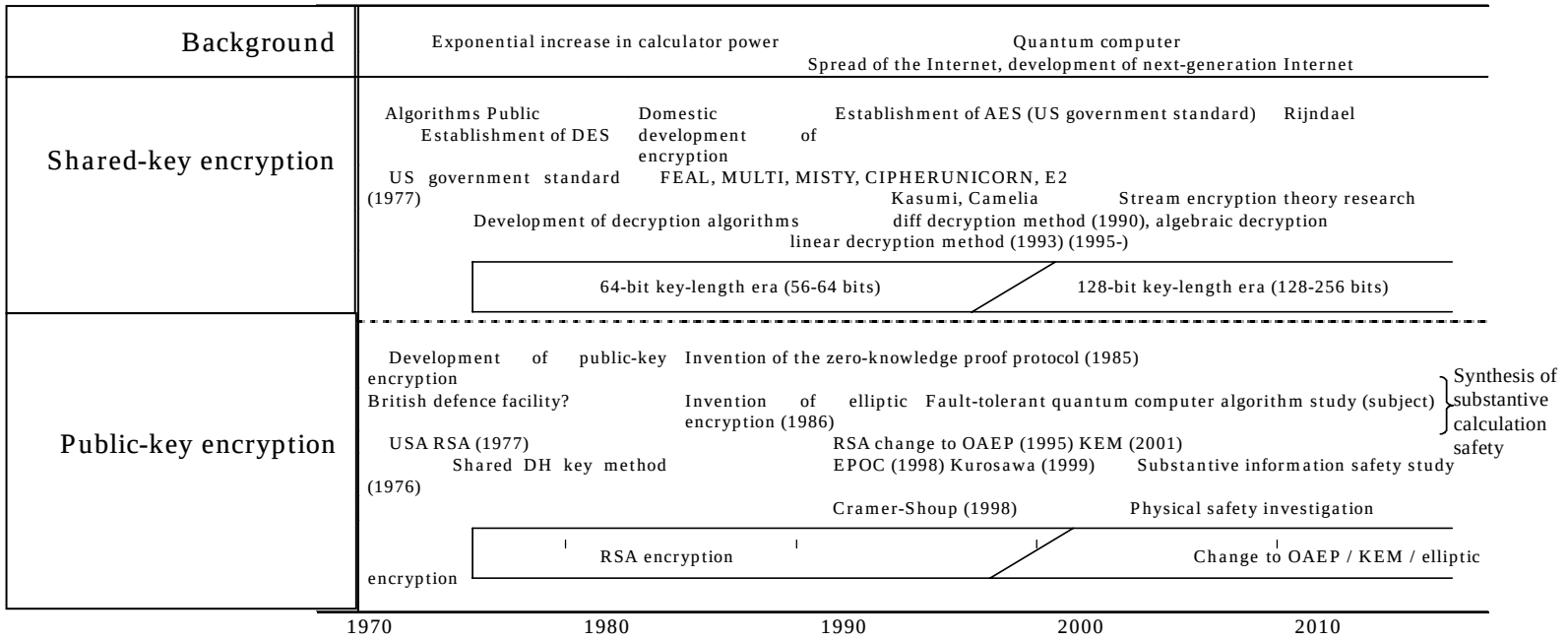

Fig. 8 Development of shared-key and public-key encryption