4-9 CRYPTREC Activities

KUROKAWA Takashi and KANAMORI Sachiko

In this paper, we show the activity of CRYPTREC between fiscal year 2006 and fiscal year 2010 in the security fundamentals group. We focus on compromise and migration of cryptographic algorithms, especially RSA1024 bit and SHA-1, and the revision of the e-Government Recommended Ciphers List.

Keywords
Cryptographic algorithm, Security evaluation, e-Government Recommended Ciphers List, Compromise, Life cycle

1 Introduction

The concept that the period from birth to death of human beings is divided into growth processes, with the repetition of them being regarded as a cycle, is called the "life cycle". A product lifecycle is a similar concept to the life cycle. For example, a product's life can be divided into four stages in relation to the sales figures of the product: introduction stage, which is a brief period after the product was launched onto the market, growth stage where the product is becoming more accepted in the market, maturity stage where the product has spread to most consumers in the market, and decline stage where the sale of the product is declining. Similarly, the life cycle of system development for information communication can be divided into five processes: planning process, requirements definition process, development process, operation process, and maintenance process.

A computer algorithm is a description of an execution procedure to compute a solution for a problem. We think that it will work permanently because its correctness is proven mathematically and then it may be inappropriate to apply the concept of life cycle to a computer algorithm. On the other hand, a cryptographic algorithm, a kind of computer algorithm, is associated with security parameters that determine the strength of security and has a lifetime in terms of assurance of security; therefore, the concept of life cycle can be applied to it naturally. Thus, ensuring the security of a cryptographic algorithm is considered as an essential action to determine its current stage in the life cycle.

2 About CRYPTREC

CRYPTREC is an abbreviation of Cryptography Research and Evaluation Committees, and it refers to a project to evaluate and monitor the security of e-Government recommended ciphers, as well as to investigate and examine the appropriate implementation/operation methods of cryptographic techniques.

It started in 2000 when the Information-Technology Promotion Agency, Japan (IPA) was commissioned a research project from the Ministry of International Trade and Industry (current Ministry of Economy, Trade and Industry) as a part of an e-Government information security technology development project, to organize an evaluation committee in order to evaluate technical aspects, such as security and performance, of cryptographic techniques applicable to e-Government, and acted as the secretariat for the committee.

Since 2001, Telecommunications Advancement Organization of Japan (which was later merged with Communications Research Laboratory to become National Institute of Information and Communications Technology (NICT)) has been participating in the joint secretariat for the committee. In addition to the committee, the Director-General for Technology Policy Coordination, Minister's Secretariat, Ministry of Internal Affairs and Communications (MIC) and the Director-General, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry (METI) established the Advisory Board for Cryptographic Technology in order to contribute specialists' opinions into the measures of the both ministries to promote information security policy by diffusing cryptographic technologies. Since FY 2008, the Director-General for Technology Policy Coordination was changed to the Director General for Secretariat's Policy Matters (both Minister's Secretariat, Ministry of Internal Affairs and Communications), which was again changed to the Director-General for Policy Planning, Ministry of Internal Affairs and Communications from FY 2010.

3 Background of the establishment of CRYPTREC

It is essential to ensure the security and reliability of information and communication technology to realize electronic commerce over telecommunication network. With the rapid expansion of the Internet worldwide, there are growing concerns about threats such as distributed denial of service (DDoS) attacks, computer viruses, illegal access, and spoofing, and cryptographic techniques have been introduced as technical countermeasures. In short, cryptographic techniques are increasingly utilized not only for the confidentiality of information but also to ensure the authenticity and integrity of information.

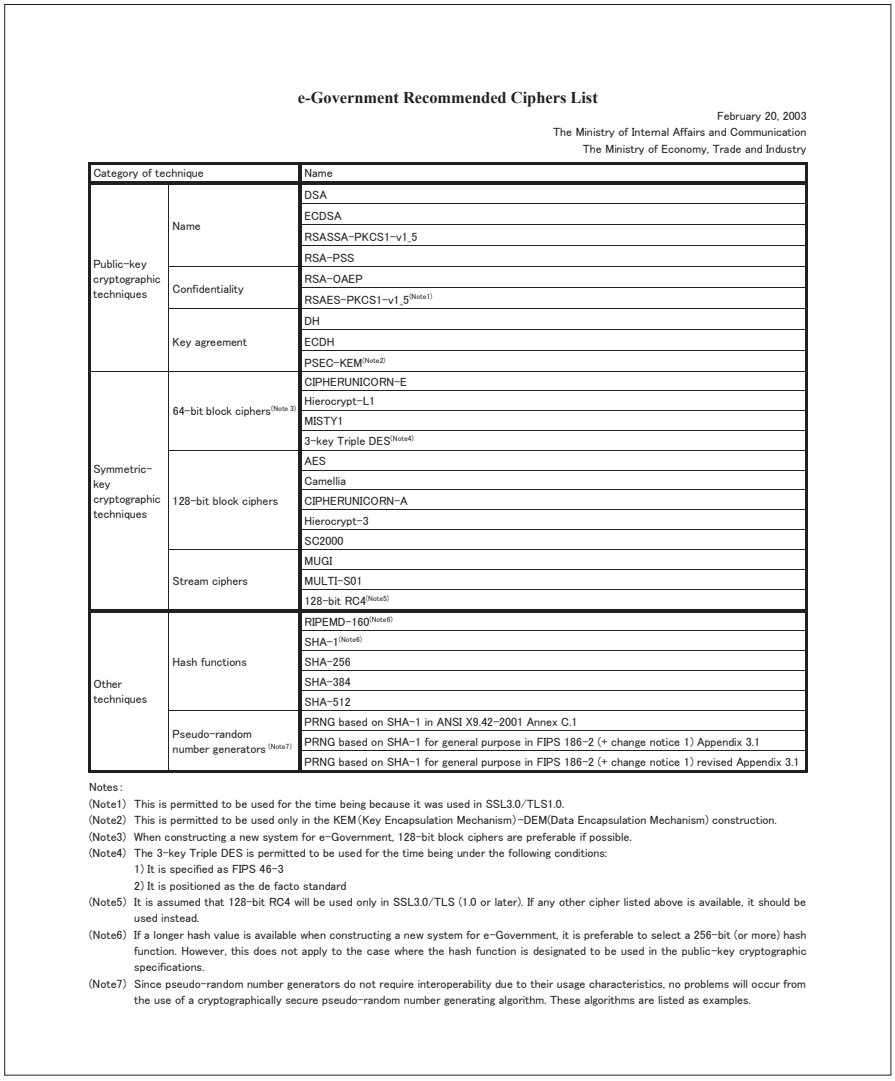
Traditionally, cryptographic techniques have been regarded as arms to protect the confidentiality of information from the standpoint of trade control; however, due to the expansion of the commercial use of the Internet, the regulations for cryptographic techniques for signature and authentication are becoming more relaxed. In addition, the National Institute of Standards and Technology (NIST) in the United States promoted a project to adopt a new Advanced Encryption Standard (AES) (from 1997 to 2000). As for the international standards, the register of cryptographic algorithm ISO 9979 started to be replaced with the standardization of cryptographic algorithm for confidentiality ISO/IEC 18033. As such, the momentum of standardization was increasing around 2000.

In terms of Japan's policy, the IT Strategy Council of the Cabinet Secretariat established the "e-Japan Priority Policy" at the end of FY 2000, the description of which includes the following: "In order to adopt cryptographic techniques with superior performance whose security has been objectively evaluated, by FY 2002 we will evaluate and standardize cryptographic techniques that will be helpful in e-government applications and the like. This will be accomplished by holding advisory committee meetings and the like involving experts, in consideration of international standardization of cryptographic techniques by organizations such as the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU)".

4 Organization of CRYPTREC

4.1 The organization until the end of FY 2008

Following the open call for cryptographic techniques in FY 2000 and FY 2001 and the evaluation of cryptographic techniques from FY 2000 to FY 2002, a list of ciphers that should be recommended for use in the procurement of "e-Government" (e-Government Recommended Ciphers List (Fig. 1)) was established and published in February, 2003. However, further activities were required in order to ensure the security and reliability, which involved collecting information and evaluating the security of each cipher on the list, as well



e-Government Recommended Ciphers List

February 20, 2003
The Ministry of Internal Affairs and Communication
The Ministry of Economy, Trade and Industry

Category of technique		Name
Public-key cryptographic techniques	Name	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	Confidentiality	RSA-OAEP
		RSAES-PKCS1-v1_5(Note1)
	Key agreement	DH
		ECDH
		PSEC-KEM(Note2)
Symmetric-key cryptographic techniques	64-bit block ciphers(Note 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(Note4)
	128-bit block ciphers	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	Stream ciphers	MUGI
		MULTI-S01
		128-bit RC4(Note5)
Other techniques	Hash functions	RIPEMD-160(Note6)
		SHA-1(Note6)
		SHA-256
		SHA-384
		SHA-512
	Pseudo-random number generators (Note7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

Notes:
(Note1) This is permitted to be used for the time being because it was used in SSL3.0/TLS1.0.
(Note2) This is permitted to be used only in the KEM (Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism) construction.
(Note3) When constructing a new system for e-Government, 128-bit block ciphers are preferable if possible.
(Note4) The 3-key Triple DES is permitted to be used for the time being under the following conditions:
1) It is specified as FIPS 46-3
2) It is positioned as the de facto standard
(Note5) It is assumed that 128-bit RC4 will be used only in SSL3.0/TLS (1.0 or later). If any other cipher listed above is available, it should be used instead.
(Note6) If a longer hash value is available when constructing a new system for e-Government, it is preferable to select a 256-bit (or more) hash function. However, this does not apply to the case where the hash function is designated to be used in the public-key cryptographic specifications.
(Note7) Since pseudo-random number generators do not require interoperability due to their usage characteristics, no problems will occur from the use of a cryptographically secure pseudo-random number generating algorithm. These algorithms are listed as examples.

Fig.1 *E-Government Recommended Ciphers List (current list)*

as announcing the updated information and making changes (including deletions) to the e-Government Recommended Ciphers List as needed. To achieve this, the organization has been reformed as described in ***4.1.1*** and ***4.1.2*** (Fig. 2).

4.1.1 Cryptographic technique monitoring subcommittee

The Cryptographic Technique Monitoring Subcommittee is positioned under the Advisory Committee; it carries out monitoring of e-Government recommended ciphers, as well as investigation/examination placing focus on cryptographic algorithms related to e-Government recommended ciphers. Also, the Cryptographic Technique Investigation WG has been established under the Subcommittee, to engage in examination activity aimed at assisting the activities of the Subcommittee. The Cryptographic Technique Monitoring Subcommittee holds session as a committee meeting of NICT and IPA, in which MIC, METI, the National Police Agency (NPA), the Ministry of Foreign Affairs (MOFA), the Ministry of Defense (MOD), etc., participate as observers (Fig. 3).

4.1.2 Cryptographic module subcommittee

The Cryptographic Module Subcommittee is positioned under the Advisory Committee; it engages in examination toward the estab-

lishment of security and test requirements for cryptographic module products conforming to e-Government recommended ciphers, paying attention to the trends of international standards, such as ISO/IEC, and considering the possibility that these requirements may be used as the standard for governmental procurement in the future. In addition, the Subcommittee investigates and examines side channel attacks and tampering in relation to implementation of cryptographic techniques, aiming to contribute to improvement of the above-mentioned security and test requirements. The Cryptographic Module Subcommittee holds session as a committee meeting of NICT and IPA, in which MIC, METI, NPA, MOFA, MOD, etc., participate as observers.

4.2 The organization from FY 2009

In preparation for the revision of e-Government Recommended Ciphers List, CRYPTREC was reformed as described in ***4.2.1–4.2.3*** in order to carry out investigation/examination focusing on the operational management of cryptographic techniques, in addition to the previous main activities of investigation/examination for assurance of security and reliability of the e-Government recommended ciphers (Fig. 4).

4.2.1 Cryptographic scheme committee

The Cryptographic Scheme Committee was established in FY 2009 to take over from the Cryptographic Technique Monitoring Subcommittee, which existed until the end of FY 2008. In addition to the previous tasks of the Cryptographic Technique Monitoring Sub-

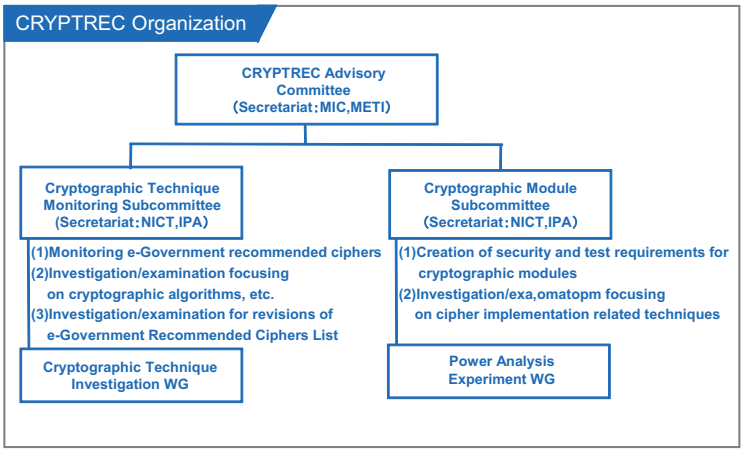


Fig.2 *The organization of CRYPTREC in FY2003-2008*

Fig.3 *Former organization of CRYPTREC*

committee, it was assigned to carry out investigation/examination of the security of cryptographic techniques in preparation for the revision of the e-Government Recommended Ciphers List, as well as investigation/examination of cryptographic techniques that will be potentially used for the e-Government in the future.

4.2.2 Cryptographic module committee

The Cryptographic Module Committee was established in FY 2009 to take over from the Cryptographic Module Subcommittee, which existed until the end of FY 2008. In addition to the previous tasks of the Cryptographic Module Subcommittee, it was assigned to carry out investigation/examination of performance evaluation in preparation for the revision of the e-Government Recommended Ciphers List.

4.2.3 Cryptographic operation committee

The Cryptographic Operation Committee was newly established in order to mainly investigate/examine the operational management of cryptographic techniques which will be required for establishment/operation of the new e-Government Recommended Ciphers List (new cipher list). Specifically, it investigates/examines appropriate operation of the e-Government recommended ciphers used for e-Government systems, etc., from the viewpoint of system designers/providers. It focuses on examination of evaluation policy/standards for evaluation of commercialization/actual use of cryptographic techniques in establishing the new list. It also examines the consistency of the e-Government Recommended Ciphers List and international standard techniques. In addition, the Committee examines the policy for handling cryptographic techniques published in the monitoring ciphers list. When migration becomes necessary due to compromise, investigation/examination will be carried out in order to enable more smooth operation from the viewpoint of the system designers/providers.

4.3 History of committee meetings

The schedule of the committee and other meetings from FY 2006 to FY 2010 is given in Table 1.

5 Notable efforts in the Second Medium-term Plan

5.1 Compromise and migration of cryptography

Compromise of a cryptographic algorithm means the situation where the security level of a cryptographic algorithm has been reduced, or the security of the system in which the affected cryptographic algorithm is incorporated has been threatened. Generally, the situation is described as “cryptographic algorithm has been broken or cracked”. There are number of methods to analyze cryptographic

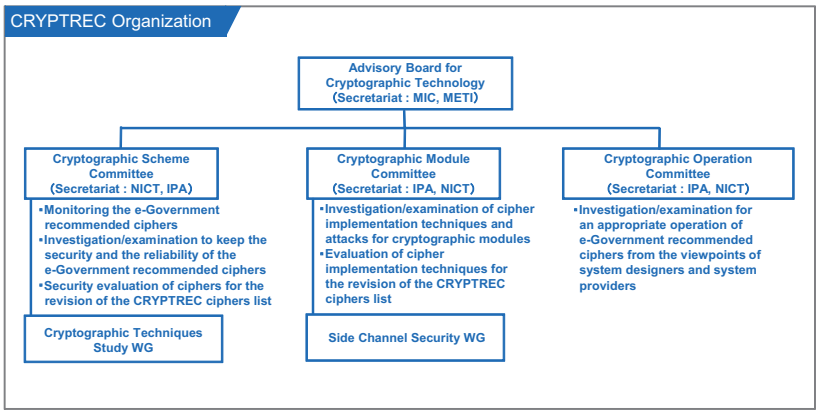


Fig.4 *The organization of CRYPTREC (FY 2009-)*

Table 1 *List of committee meetings held in the Second Medium-term Plan*

	Fiscal Year Ended March 31, 2006		Fiscal Year Ended March 31, 2007		Fiscal Year Ended March 31, 2008	
Cryptographic Technique Monitoring Subcommittee	The 1st	July 24, 2006	The 1st	June 5, 2007	The 1st	July 28, 2008
	The 2nd	March 9, 2007	The 2nd	November 13, 2007	The 2nd	October 28, 2008
			The 3rd	March 3, 2008	The 3rd	December 19, 2008
					The 4th	March 4, 2009
Cryptographic Technique Investigation WG (Public-key)	The 1st	August 4, 2006	The 1st	May 16, 2007		
	The 2nd	September 7, 2006	The 2nd	December 18, 2007		
	The 3rd	December 27, 2006	The 3rd	February 8, 2008		
	The 4th	February 5, 2007	The 4th	February 22, 2008		
	The 5th	February 5, 2007				
	The 6th	March 7, 2007				
Cryptographic Technique Investigation WG (List Guide)			The 1st	August 7, 2007	The 1st	September 2, 2008
			The 2nd	October 17, 2007	The 2nd	November 28, 2008
			The 3rd	January 16, 2008	The 3rd	January 9, 2009
			The 4th	February 25, 2008	The 4th	March 3, 2009
Cryptographic Technique Investigation WG (ID Base)			The 1st	August 7, 2007	The 1st	September 11, 2008
			The 2nd	October 17, 2007	The 2nd	November 20, 2008
			The 3rd	January 16, 2008	The 3rd	December 18, 2008
			The 4th	February 25, 2008	The 4th	February 17, 2009
Cryptographic Module Subcommittee	The 1st	July 26, 2006	The 1st	June 6, 2007	The 1st	August 1, 2008
	The 2nd	December 15, 2006	The 2nd	July 25, 2007	The 2nd	October 31, 2008
	The 3rd	March 15, 2007	The 3rd	September 28, 2007	The 3rd	December 15, 2008
			The 4th	February 15, 2008	The 4th	February 20, 2009
Power Analysis Experiment WG	The 1st	December 27, 2006	The 1st	June 27, 2007	The 1st	September 3, 2008
	The 2nd	March 2, 2007	The 2nd	October 5, 2007	The 2nd	October 3, 2008
			The 3rd	December 21, 2007	The 3rd	November 26, 2008
			The 4th	February 6, 2008	The 4th	February 4, 2009

	Fiscal Year Ended March 31, 2009		Fiscal Year Ended March 31, 2010	
Cryptographic Scheme Commmittee	The 1st	August 5, 2009	The 1st	July 20, 2010
	The 2nd	February 18, 2010	The 2nd	February 10, 2011
	The 3rd*	March 2 to 3, 2010	The 3rd*	March 2, 2011
Cryptographic Techniques Study WG (List Guide)	The 1st	September 1, 2009	The 1st	September 27, 2010
	The 2nd	October 22, 2009	The 2nd	December 2, 2010
	The 3rd	February 4, 2010	The 3rd	February 4, 2011
	The 4th*	March 2 to 3, 2010	The 4th*	March 2, 2011
Cryptographic Module Committee	The 1st	August 5, 2009	The 1st	July 23, 2010
	The 2nd	October 2, 2009	The 2nd	September 28, 2010
	The 3rd	February 24, 2010	The 3rd	February 4, 2011
	The 4th*	March 2 to 3, 2010	The 4th*	March 2, 2011
Side Channel Security WG	The 1st	September 2, 2009	The 1st*	March 2, 2011
	The 2nd	February 5, 2010		
	The 3rd*	March 2 to 3, 2010		
Cryptographic Operation Committee	The 1st	October 23, 2009	The 1st	September 14, 2010
	The 2nd	February 22, 2010	The 2nd	November 4, 2010
	The 3rd*	March 2, 2011	The 3rd	January 20, 2011
			The 4th	February 24, 2011
			The 5th*	March 2, 2011

*: Joint Meeting

algorithms, and the degree of damage of the broken/cracked cryptographic algorithm can be only determined when more details are provided.

The security level of cryptographic algorithms is divided into the following four states.

- State 1: There is no known efficient attack exploiting the flaw in the cryptographic algorithm.
- State 2: Although an attack exploiting the flaw in the cryptographic algorithm has been proposed, the attack is only partially successful and the algorithm has not been academically broken.
- State 3: An attack exploiting the flaw in the cryptographic algorithm has been proposed, and the algorithm has been academically broken.
- State 4: An attack that could be a practical threat to actual systems and applications utilizing the cryptographic algorithm has been presented.

Among these, the state of a "partially successful attack" in State 2 means that, in the case of asymmetric ciphers, a drawback breaking a mathematical problem on which the security depends has been found but the security of the cryptographic algorithm itself is not under

threat, or in the case of symmetric ciphers, some conditions are required to apply the attack, such as the need to modify the functions or number of steps in the cryptographic algorithms, or the need to obtain a vast amount of plain text/cipher text pairs.

Most of the attacks categorized in State 3 mean that a vast amount of plain text/cipher text pairs are required to apply the attacks, or even if the algorithm has been "academically broken", some countermeasures can be taken against the attacks, such as updating the key more frequently.

In addition, State 4 means that the attack can be applied to some applications with the computing power of a mid-scale laboratory*1, and an advantage of a cryptographic algorithm for security has been lost.

Generally, a cryptographic algorithm is not used individually, but functions as a part of software/hardware when it is incorporated into a system.

The issue of compromise is whether it is possible to replace cryptographic algorithms or change their parameter settings when a cryptographic algorithm used in a system has been compromised. Unfortunately, there are very few cases where systems are constructed with consideration of changes of cryptographic algorithms.

5.1.1 Compromise of RSA1024 bit

The factoring problem is defined as a problem where, when a composite number N, the product of two primes p and q which are different from each other and unknown, are given, the divisors p and q should be found only from N. The RSA algorithm is a kind of public key cryptography published by Rivest, Shamir and Adleman in 1978, the security of which depends on the difficulty of the factoring problem. Since breaking a private key from a public key could enable decryption of cipher text and forgery of signature, the difficulty of factoring problem has a meaningful place to select an RSA modulus. Around 1990, mathematicians such as Pollard proposed the General Number Field Sieve (GNFS), and since then the size of composite number that can be decomposed is gradually becoming larger. GNFS is an algorithm that finds the following nontrivial representation

$$x^2 \equiv y^2 \pmod{N}$$

and computes the greatest common divisor $\mathrm{GCD}(x \pm y, N)$ to find the divisors of N. GNFS consists of five steps: selecting a polynomial, collecting relations, filtering, computing a system of linear equations, and computing a square root. Most of the computational cost consists of collecting relations and computing a system of linear equations. It is the fastest algorithm known to this day, and one of the characteristics is the complicated parameter setting for optimization.

CRYPTREC set up the Public Key Cryptography WG under the Cryptographic Technique Monitoring Subcommittee, and conducted investigation/examination of the computational cost of the difficulty of the factoring problem. The result is shown in Fig. 5.

5.1.2 Compromise of SHA-1

The security of a hash function H is generally divided into the following three categories.

(1) Collision resistance — difficulty to find message M_1 and M_2 where the corresponding hash values are equal to each other, that is $\mathrm{H}(M_1) = \mathrm{H}(M_2)$.
(2) Second preimage resistance — when a known message M and the hash value corresponding to the message are given, it is difficult to find a different message M' that has the same hash value, that is $\mathrm{H}(M) = \mathrm{H}(M')$.
(3) Preimage resistance — when a hash value corresponding to an unknown message M is given, it is difficult to find message M' that has the same hash value, that is $\mathrm{H}(M) = \mathrm{H}(M')$.

However, with the progress of research on the method to find MD5 collisions, Arjen Lenstra's research team succeeded in forging intermediate CA certificates by actually mak-

*1 Based on a "Corporate Department" computing environment prepared with 30,000 dollars budget, as described in Blaze et al.[1996].

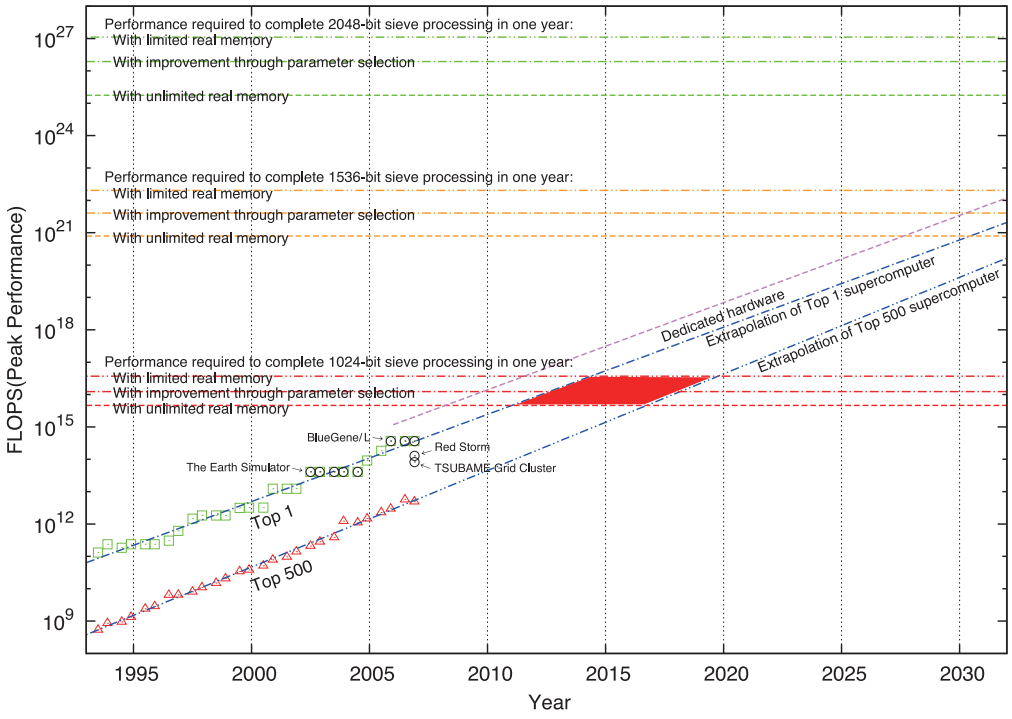


Fig.5 *Estimate of the required computer processing performance to complete the step to collect relational expression in one year*

ing a commercial CA sign the forged X.509 certificate, in terms of the hash function MD5 (Fig. 6).

The important point is that the following new search algorithm that is different from the above (1)–(3) has been proposed.

(4) Chosen-prefix collision resistance — when known messages P_1 and P_2 are given, it is difficult to compute messages S_1 and S_2 where the corresponding hash values match each other, that is $H(P_1 \| S_1) = H(P_2 \| S_2)$.

This search algorithm enables the forging of X.509 certificates by using MD5 in more realistic situations, even if the function has second preimage resistance.

SHA-1 is a 160-bit hash function with 512-bit block length and 160-bit hash length, which was established by NIST of the United States in 1995. No serious issue has been found for about 10 years since its proposal, however, Xiaoyun Wang et al., who also discovered MD5 collisions, proposed a collision search algorithm in 2005. According to the evaluation by Wang in 2005, the computational cost of finding collisions was in a range of 2^{63}–2^{69}. Using the same format as the factoring problem, compromise of SHA-1 is shown in Fig. 7. However, vulnerability against chosen-prefix collision resistance has not been found for SHA-1.

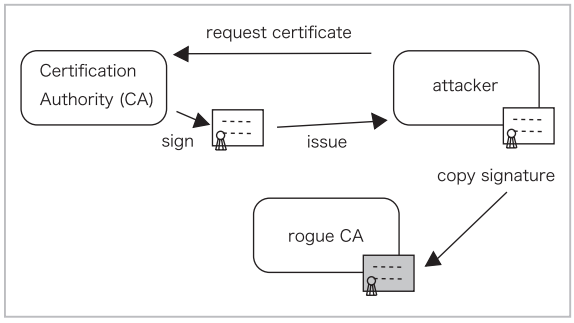


Fig.6 *Schematic diagram of intermediate CA certificates being forged*

5.1.3 Migration of cryptography

In order for a life cycle of an information communication system using cryptographic technology to make sense as a cycle, migration of cryptography needs to be taken account of

when renewing the system. In that case, it is very important to examine the migration policy of cryptographic algorithms and the roadmap of the migration in order to examine how to enforce the change of cryptographic algorithms.

As described in ***5.1.2***, CRYPTREC published the evaluation result of collision resistance of SHA-1 in 2005 and the evaluation result of the difficulty of the factoring problem in RSA1024 bit in 2006. Following these, in FY 2008, National Information Security Center (NISC), the organization to formulate/implement information security measures related to governmental information systems, established the migration policy for SHA-1 and RSA1024 bit that is used for governmental information systems (Fig. 8). The policy has adopted government-wide countermeasures that aim to develop a system where SHA-256 and RSA2048 bit will be available to select in accordance with the life cycle, including sys-

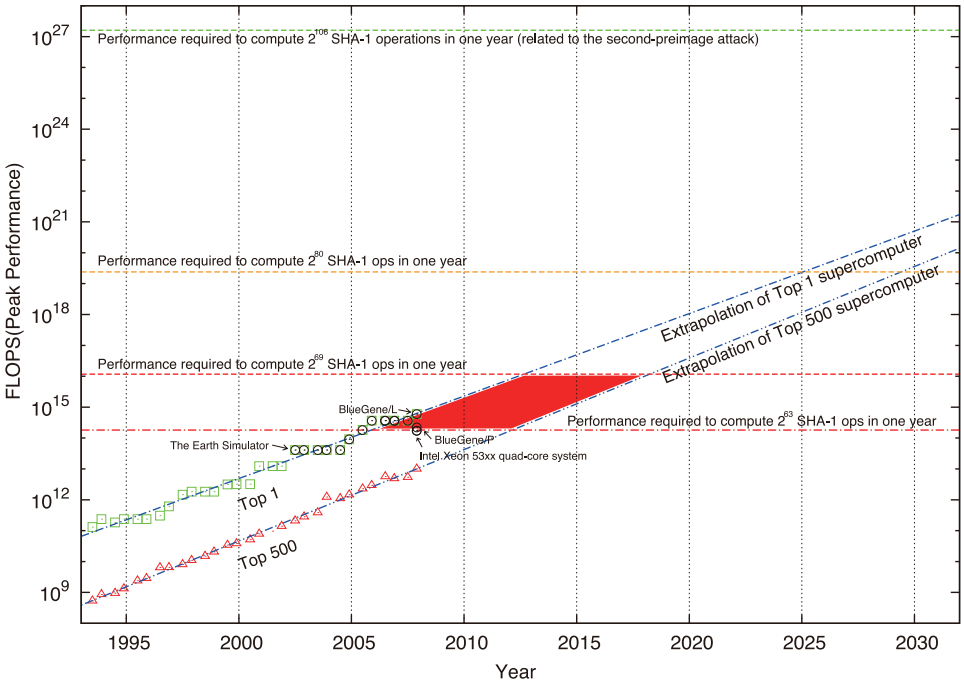


Fig.7 *Estimate of computational cost of attack against SHA-1*

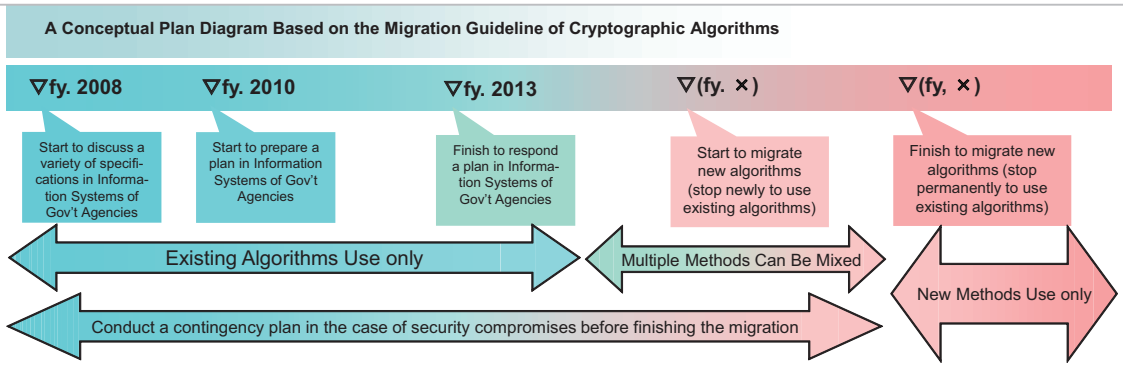


Fig.8 *A conceptual plan diagram based on the migration guideline of cryptographic algorithms*

Citation: NISC, Decision of "Migration Plan of Cryptographic Algorithm SHA-1 and RSA1024 in Information Systems of Government Agencies"

tem renewal, of e-Government systems of each governmental department, such as Government Public Key Infrastructure (GPKI).

The length of period required for the migration depends on the timing of system renewal; however, it will be very rare that a budget is allocated immediately and the migration is completed within a few years, so in most cases it should be seen over a longer span of time, from 5–10 years. Therefore, the security of cryptographic techniques needs to be maintained for at least 15–20 years.

5.2 Response to the requirements from JCMVP

CRYPTREC has received a request from the secretariat of Japan Cryptographic Module Validation Program (JCMVP) of IPA that pointed out there were some specification differences between the cryptographic techniques published in the e-Government Recommended Ciphers List and the security functions approved by JCMVP and asked us to authorize the JCMVP's specification as well. In order to approve the request, we needed to examine the validity of the changes (including additions) to the reference of the specification documents or the changes to the specification documents. In FY 2007, after obtaining approval from Advisory Board for Cryptographic Technology, the Public Key Cryptography WG under the Cryptographic Technique Monitoring Subcommittee investigated/examined the security of the following items.

- Key Derivation Function (KDF function) related to DH and ECDH
- Generation/verification of elliptic curve domain parameters related to ECDSA and ECDH
- PSEC-KEM related to the specification changes that occurred in accordance with ISO standardization

Since CRYPTREC's activities have been based on the concept of transmitting information mainly for e-Government, there is a lack of information on what will become important when transmitting information for not only JCMVP, but also organizations other than government, especially the private sector. This will be an issue in the future.

5.3 Revision of the e-Government Recommended Ciphers List

In FY 2000, we issued a public call and started evaluation activity to select cryptographic techniques which are judged to have superior security and performance by objective evaluation. We published the e-Government Recommended Ciphers List (current list) at the end of FY 2002, then since FY 2003 we have been conducting monitoring activity as well as evaluation of security. At present, analysis/attack technologies against cryptographic techniques are becoming more advanced, and development of new cryptographic techniques is progressing. In addition to this, since the ciphers adopted for the current list are based on the concept that they can be securely used for 10 years after the establishment of the list, it is necessary to revise the list in FY 2012 (Fig. 9).

5.3.1 The draft outline for revision of e-Government Recommended Ciphers List

In order to revise the e-Government recommended ciphers, we solicited comments from the general public in FY 2008, which was entitled as "The Draft Outline for Revision of the e-Government Recommended Ciphers List".

The structure of the current list was reviewed based on a cryptographic life cycle, simulating from the development to compromise of a cipher, and it was decided to publish the following lists (1)–(3) and a list guide (4) under the name of "CRYPTREC Ciphers List (provisional title)" (new list).

(1) e-Government Recommended Ciphers List
(2) Recommended Cipher Candidates List
(3) Monitored Ciphers List
(4) List Guide

Once the security has been confirmed by CRYPTREC, the cryptographic techniques will be registered to one of the three lists (1)–(3). The registration is determined according to the security and market trends, with con-

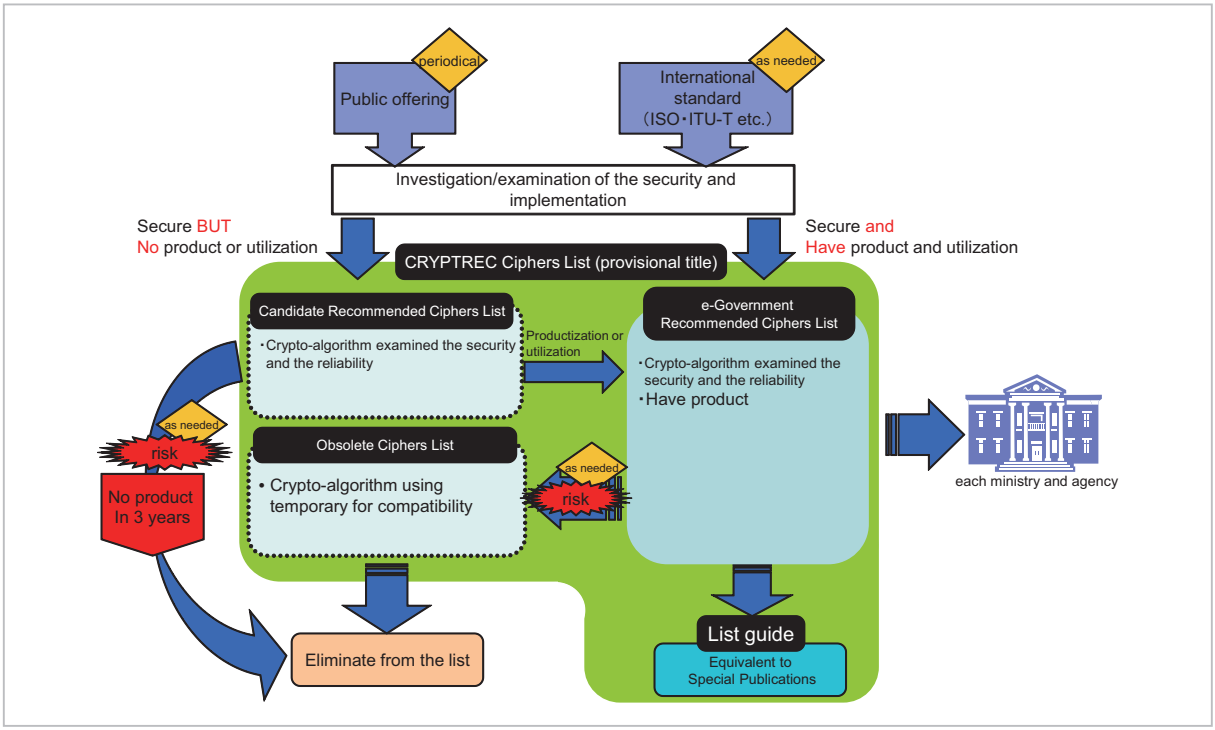


Fig.9 *Image of revised list*

Ref: public comment of "The revise of the e-Government Recommended Ciphers List" 2008

sideration given to consistency with the WTO Agreement on Government Procurement. The registration is reviewed at regular intervals. The security of the cryptographic techniques in the current list will be re-evaluated, and these techniques will be regarded as registered in the Recommended Cipher Candidates List until the new list takes effect in 2013. Once the operation of the new list starts in 2013, whether these techniques should be registered to the e-Government Recommended Ciphers List will be determined together with the newly applied techniques, in accordance with the status of commercialization and their actual use.

The role of each (partial) list in the new list is as follows.

(1) e-Government Recommended Ciphers List

The list of techniques for which security has been confirmed by CRYPTREC, and that have a proven track record of use in the market. These techniques are recommended for construction of e-Government (governmental procurement) (equivalent to the current list). It is desirable that the techniques registered in this list are standardized by organizations like ISO.

(2) Recommended Cipher Candidates List

The list of techniques for which security has been confirmed by CRYPTREC, but that do not have sufficient track record of use in the market. It includes new techniques for which use is expected to grow in future. These techniques may be used for construction of e-Government (governmental procurement). The degree of their diffusion will be investigated at regular intervals, and if it is recognized that they have sufficient track record of use, they will be registered to the e-Government Recommended Ciphers List. On the other hand, if sufficient track record has not been recognized, they will be removed from this list. In addition, when a cryptographic technique has become no longer appropriate for recommendation, such as when the risk of being deciphered has increased, that cryptographic technique will be deleted from the list as needed.

(3) Monitored Ciphers List

The list of techniques for which use is permitted only for the purpose of maintaining compatibility. These techniques were previ-

ously registered in the e-Government Recommended Ciphers List, but are no longer recommended due to the increased risk of being deciphered. Whether to keep them in the list is judged regularly based on the risk of being deciphered and the cost of migration in the e-Government. CRYPTREC does not recommend new procurement of these techniques.

(4) List Guide

Summary of the techniques which are used or will be potentially used for e-Government, and the description of their usage. It also describes specific parameter settings for the techniques in the new list that require correct setting of parameters to maintain the security. In addition, it describes the state of development and applicability of security technology that is expected to be needed in the future. The List Guide aims to be used by system providers or designers, and to educate system users.

Basic policy for open call for cryptographic techniques

The basic policy for the open call was as follows.

(1) The categories of application should satisfy one of the following conditions (1a)–(1c).
  (1a) A cryptographic technique category that is not in the current list, but requires recommendation of technical specification with superior security and performance for constructing e-Government systems.
  (1b) A cryptographic technique category that has more advantages than the cryptographic algorithms in the current list, and in which new techniques have been proposed in international conferences.
  (1c) A cryptographic technique category for which diffusion/standardization can be expected.

(2) The submitted cryptographic techniques should satisfy all of the following conditions (2a)–(2e).
  (2a) The cryptographic technique should have sufficient security. However, if it belongs to the same category as the cryptographic techniques in the current list, it should be superior in terms of security or performance.
  (2b) The cryptographic technique should be versatile and should not be dependent on individual systems or specification of an application.
  (2c) A product that uses the technique has been on sale or is planned to be on sale.
  (2d) The technical specification that satisfies the evaluation criteria of security and performance has been published.
  (2e) In terms of the basic patents of the cryptographic technique, the licensing rights of the technique for production, sales and use should be given royalty free or under reasonable and non-discriminatory conditions.

5.3.2 Open call for cryptographic techniques towards the revision of the e-Government Recommended Ciphers List (FY 2009)

Outline of the open call

The policy of the open call included the following conditions: a cryptographic technique category that has more advantages than the cryptographic algorithms in the current list, and where new techniques have been proposed in international conferences, and, as for a cryptographic technique that belongs to the same category as those in the current list, it should be superior in terms of security or performance. When conducting evaluation of cryptographic techniques, we will organize the characteristics of security and performance of each technique based on the evaluation commissioned to domestic/international specialists with proven experience in the field and the evaluation published in conferences and papers.

Application categories

The application categories of cryptographic techniques for the FY 2009 open call are shown in Table 2. However, the following considerations needed to be taken into account.

- The submitted cryptographic technique has been published in peer-reviewed international conferences or peer-reviewed international papers, or has been accepted by the end of September 2010.

- The intellectual property can be used free of charge when evaluating the technique.
- The submitted cryptographic technique or products that use the technique can be provided within three years of the establishment of the new list in order to be used for e-Government.

Application period

October 1, 2009 – February 4, 2010, 17:00

Submitted cryptographic techniques

We received the following six applications as shown in Table 3 for the FY 2009 open call.

The cryptographic techniques selected by the secretariat

The CRYPTREC Secretariat adopted the following cryptographic techniques which have been standardized internationally, referring to the result of examinations that were conducted by CRYPTREC when the List Guide was established (Table 4).

Evaluation schedule for the submitted cryptographic techniques

The submitted cryptographic techniques will be evaluated toward the revision of the e-Government Recommended Ciphers List in FY 2012. The schedule is as Fig. 10. In 2010, we conducted evaluation focusing on the submitted cryptographic techniques. In 2011, we will continue the evaluation of the submitted techniques and at the same time will re-evaluate the techniques in the current list. Based on the evaluation result, the Cryptographic Scheme Committee and the Cryptographic Module Committee will judge whether or not to include the techniques in the "CRYPTREC Ciphers List (provisional title)" and submit a report to the Advisory Board for Cryptographic Technology. The content of the report will be discussed in the Advisory Board for Cryptographic Technology, and then the final decision will be made by the Ministry of Inter-

Table 2 *Specification of solicited cryptographic techniques in FY 2009*

Category	Specification
Block Cipher	The block size of plain text and cipher text is 128 bit length. It supports 128 bit, 192 bit and 256 bit as key length. It has no less features (as security or performance) than cryptographic techniques listed in the existing e-Government Recommended Ciphers List will have.
Mode of Operation	Block cipher modes of operation for 128 bit block cipher and 64 bit block cipher.
Message Authentication Code	Message authentication code using 128 bit block cipher and 64 bit block cipher with 128 bit key length.
Stream Cipher	Stream cipher encrypts plain texts by a bit or a byte. Its key length is 128 bit or longer.
Entity Authentication	Entity authentication composed of symmetric ciphers, asymmetric ciphers, hash functions, message authentication code listed in the existing e-Government Recommended Ciphers List or entity authentication the security of which can be reduced to a computational hardness assumptions. As a general rule, primitives composing an entity authentication shall be listed in the existing e-Government recommended ciphers. When you use symmetric ciphers, message authentication codes not listed in the existing e-Government recommended ciphers as a primitive, you need to submit it simultaneously. And you can submit an entity authentication using any primitives not mentioned above.

Table 3 *List of submitted cryptographic techniques in FY 2009*

Category	Name of cryptographic technique	Applicant
128 bit Block Cipher	CLEFIA	HyRAL
	HyRAL	Laurel Intelligent Systems Co., Ltd.
Stream Cipher	Enocoro-128v2	Hitachi, Ltd.
	KCipher-2	KDDI Corporation
Message Authentication Code	PC-MAC-AES	NEC Corporation
Entity Authentication	Infinite One-Time Password	Nihon Unisys Ltd.

There are no applicants for the category of modes of operation.

Table 4 *List of cryptographic techniques that were selected to be evaluated by CRYPTREC Secretariat in FY 2009*

Category	Name of cryptographic technique	Specification
Message Authentication Code (Selected by the "List Guide WG" (a cryptographic techniques study working group)	CBC-MAC	ISO/IEC 9797-1
	CMAC	NIST SP 800-38B
	HMAC	NIST FIPS 198-1
Modes of Operation (Selected by the "List Guide WG" (a cryptographic techniques study working group)	CBC Mode	NIST SP 800-38A
	CFB Mode	NIST SP 800-38A
	OFB Mode	NIST SP 800-38A
	CTR Mode	NIST SP 800-38A
	GCM Mode	NIST SP 800-38C
	CCM Mode	NIST SP 800-38C
Entity Authentication (Selected in view of standardization trends)	Authentication protocol using symmetric ciphers	ISO/IEC 9798-2, Mechanisms using symmetric encipherment algorithms
	Authentication protocol using electronic signature schemes	ISO/IEC 9798-3, Mechanisms using digital signature techniques
	Authentication protocol using a check function (MAC)	ISO/IEC 9798-4, Mechanisms using a cryptographic check function

There are no selections for the category of 128 bit block cipher and stream cipher.

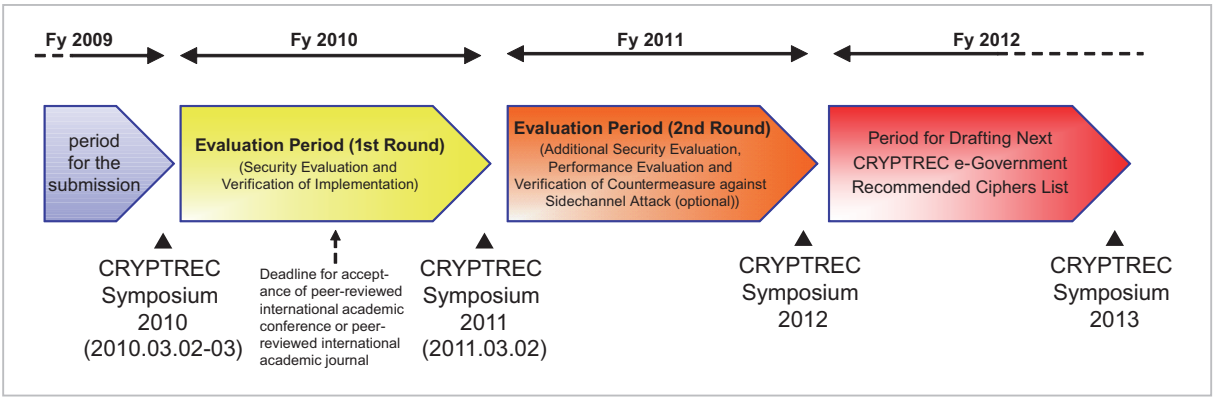


Fig.10 *Evaluation schedule*

Citation: Guidance for submissions of Cryptographic Techniques for revision of the e-Government Recommended Ciphers List (FY 2009)

nal Affairs and Communication and the Ministry of Economy, Trade and Industry. The decision will be made in FY 2012.

Evaluation items of the submitted cryptographic techniques

There are mainly two categories: evaluation items for security and evaluation items for performance.

(1) Evaluation items for security

Evaluate resistance to the known typical attacks. The evaluation may include a specific attack against a particular cipher, or grounds for heuristic security.

(2) Evaluation items for performance

Confirm the feasibility based on the submitted materials. Software implementation is evaluated by the performance (processing speed, memory usage) on a standard platform. Hardware implementation (except entity authentication) is evaluated by the performance (processing speed, the number of used cells or gates) of each used process (FPGA*2, ASIC*3, etc.). In addition, the feasibility of countermeasures against side channel attacks will be confirmed for some cryptographic techniques.

*2 FPGA: Field Programmable Gate Array
*3 ASIC: Application Specific Integrated Circuit

5.3.3 The Progress of the first evaluation (FY 2010)

Submitted cryptographic techniques

Table 5 *Evaluation result of the submitted cryptographic techniques in the 1st round*

Category	Name of cryptographic technique	Applicant	Evaluation results in the 1st round
128 bit block cipher	CLEFIA	Sony Corporation	Move on to the 2nd round evaluation
	Sony Corporation	Laurel Intelligent Systems Co., Ltd.	At present, there are no security flaws between 128 bit key length and 255 bit key length. In 256 bit key length, a very small number of equivalent keys and a computationally feasible derivation method for them are found. Consequently, we decided that it did not have no less features than cryptographic techniques listed in the existing e-Government Recommended Ciphers List would have and finished its evaluation at 1st round and would not listed it in the next e-government recommend list.
Stream cipher	Enocoro-128v2	Hitachi, Ltd.	Move on to the 2nd round evaluation
	KCipher-2	KDDI Corporation	Move on to the 2nd round evaluation
Message Authentication Code	PC-MAC-AES	NEC Corporation	Move on to the 2nd round evaluation

† There are no applicants for the category of modes of operation.
‡ Infinite One-Time Password, submitted to the category of entity authentication, lost an application qualification because it was not accepted to any peer-reviewed international academic conferences or any peer-reviewed international academic journals till the end of September 2010.

The cryptographic techniques adopted by the secretariat

Table 6 *Evaluation result of the selected cryptographic techniques in the 1st round*

Category	Name of cryptographic technique	Specification	Evaluation results in the 1st round
Evaluation results in the 1st round	CBC-MAC	ISO/IEC 9797-1	These techniques will be listed by the next e-Government Recommended Ciphers List after considering alarming uses and comments for their use.
	CMAC	NIST SP 800-38B	
	HMAC	NIST FIPS 198-1	
Modes of Operation	CBC Mode	NIST SP 800-38A	
	CFB Mode	NIST SP 800-38A	
	OFB Mode	NIST SP 800-38A	
	CTR Mode	NIST SP 800-38A	
	GCM Mode	NIST SP 800-38C	
	CCM Mode	NIST SP 800-38C	
Entity Authentication	Authentication protocol using symmetric ciphers	ISO/IEC 9798-2, Mechanisms using symmetric encipherment algorithms	Because security flaws were found in a part of protocol types, they will be listed by the next e-Government Recommended Ciphers List after commenting on avoidance of their use. However, because there exits fixes in a part of protocol types in which flaws were found, we will propose changes to them for ISO/IEC and reexamine the comments as soon as their fixes are done.
	Authentication protocol using digital signature schemes	ISO/IEC 9798-3, Mechanisms using digital signature techniques	
	Authentication protocol using a check function (MAC)	ISO/IEC 9798-4, Mechanisms using a cryptographic check function	

There are no selections for the category of 128 bit block cipher and stream cipher.

6 Future tasks

In terms of security evaluation, it is becoming necessary to examine security evaluation of key expansion functions, such as key related attacks against symmetric ciphers, and re-evaluation of the cryptographic techniques in the current list.

In addition, in terms of evaluation of performance, although we have experience of

establishing the current list regarding evaluation of performance, due to the significant increase of the number of subjects of evaluation and many tasks we have to conduct for the first time, such as power analysis in relation to side channel attacks, difficulties are expected in the actual work.

7 Summary

It is important to take account of security when deploying not only information and communication technology but also scientific technology to the society. In terms of information and communication technology, even though the loss of the security may not directly harm human life or body, once trust has been lost, financial loss will be caused, which will increase in accordance with the scale. When a cryptographic technique has been compromised, it needs to be determined when and how the technique should be migrated, by comparing the cost of migration and financial loss. The final decision can be made only by the organization/company that provides/manages the information and telecommunications system, not by an evaluation organization like CRYPTREC.

CRYPTREC has been conducting evaluations focusing on the security and performance of cryptographic techniques; however, since the establishment of the Cryptographic Operation Committee in FY2010, we started investigation/examination of appropriate operation of the e-Government recommended ciphers that are used for e-Government systems from the viewpoint of system designers/providers. Although the accumulation of knowledge is not a fast process, we would like to continue our examination over the coming years and make efforts to provide more useful information for system designers/providers in the future.

Acknowledgements

We would like to take this opportunity to express our gratitude to all the people who participated in CRYPTREC activities and cooperated in examinations of security and performance evaluations of cryptographic algorithms.

References

1 National Institute of Information and Communications Technology and Information Promotion Agency, Japan, "CRYPTREC Report 2005," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2006. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

2 National Institute of Information and Communications Technology and Information Promotion Agency, Japan, "CRYPTREC Report 2006," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2007. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

3 National Institute of Information and Communications Technology and Information Promotion Agency, Japan, "CRYPTREC Report 2007," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2008. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

4 National Institute of Information and Communications Technology and Information Promotion Agency, Japan, "CRYPTREC Report 2008," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2009. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

5 National Institute of Information and Communications Technology and Information Promotion Agency, Japan, “CRYPTREC Report 2009,” National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2010. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html
6 National Institute of Information and Communications Technology and Information Promotion Agency, Japan, “CRYPTREC Report 2010,” National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2011. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html
7 Ministry of Internal Affairs and Communications, Ministry of Justice, and Ministry of Economy, Trade and Industry, “Report of the Advisory Board on the Enforcement Status of the Law Concerning Electronic Signatures and Certification Services,” March 2008. (In Japanese)
Available at http://www.soumu.go.jp/menu_news/s-news/2008/080530_4.html
8 Information Security Policy Council, “Migration Plan of Cryptographic Algorithm SHA-1 and RSA1024 in Information Systems of Government Agencies,” Information Security Policy Council, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society, April 2008. (In Japanese)
Available at http://www.nisc.go.jp/active/general/res_niscrypt.html
9 Takashi Kurokawa, “Compromise of cryptographic algorithms,” JPNIC News letter, No. 44, JPNIC, pp. 64–68, March 2010. (In Japanese)
10 Masashi Une, Takashi Kurokawa, Masataka Suzuki, and Hidema Tanaka, “Practical understanding on the results of the security evaluation of cryptographic algorithms,” Kin’yu Kenkyu, Vol. 29, No. 2, Institute for Monetary and Economic Studies, Bank of Japan, pp. 201–228, April 2010. (In Japanese)
11 Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, and Michael Wiener,“Minimal Key Length for Symmetric Ciphers to Provide Adequate Commercial Security,” A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, January 1996.
12 Marc Stevens, Arjen Lenstra, and Benne de Weger, “Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities,” Eurocrypt 2007, LNCS 4515, International Association for Cryptology Research, pp. 1–22, 2007.

(Accepted June 15, 2011)

KUROKAWA Takashi
Technical Expert, Security Fundamentals Laboratory, Network Security Research Institute

KANAMORI Sachiko
Technical Expert, Security Fundamentals Laboratory, Network Security Research Institute