7-3 CRYPTREC Activities and a Revision of the e-Government Recommended Ciphers List

Takashi KUROKAWA, Sachiko KANAMORI, Ryo NOJIMA, Miyako OHKUBO, and Shiho MORIAI

In this paper, we show activities of CRYPTREC carried out by the security fundamentals laboratory between fiscal year 2011 and fiscal year 2015. We focus on "CRYPTREC Ciphers List" revised in fiscal year 2012 which has been issued as the "e-Government Recommended Ciphers List" since fiscal year 2002. We also note an outline of the present activities.

1 Introduction

CRYPTREC is an acronym for Cryptography Research and Evaluation Committees. This project evaluates and monitors the security of cryptographic technology, and surveys and studies appropriate implementation methods and operation methods for cryptographic technology. The work to amend the e-Government Recommended Ciphers List[*1] started during the 2nd Medium-term Plan was done in both the 2nd and 3rd Medium-term Plan. After the amending of the e-Government Recommended Ciphers List, CRYPTREC's organization was changed, and the content of its activities also changed. This paper first describes CRYPTEC's organization in Section **2**. Next, Section **3** describes the amendment of the e-Government Recommended Ciphers List. Section **4** describes the activities in the 3rd Medium-term Plan. Finally, future issues are discussed.

2 Organization of CRYPTEC

2.1 Organization from Fiscal 2009 to Fiscal 2012

Towards amendment of the e-Government Recommended Ciphers List, CRYPTEC was reorganized starting in fiscal 2009, as shown in Fig. 1. The activities of the Cryptographic Scheme Committee mainly handled by the Security Fundamentals Laboratory are described below.

Cryptographic Scheme Committee

This committee monitors the security of cryptographic technology included in the e-Government Recommended Ciphers List, evaluates the security of cryptographic technology for amendment of the e-Government Recommended Ciphers List, and surveys and studies cryptographic technology expected to be used in e-Government.

Cryptographic Module Committee[*2]

This committee creates security requirements and testing requirements for cryptographic modules that comply with the e-Government Recommended Ciphers, and surveys and studies evaluations of implementation aspects for amendment of the e-Government Recommended Ciphers List.

Cryptographic Operation Committee[*2]

This committee has been set up to create the new e-Government Recommended Ciphers List (hereinafter referred to as the CRYPTREC Ciphers List[*3]), and it conducts surveys and studies on the appropriate operation of the

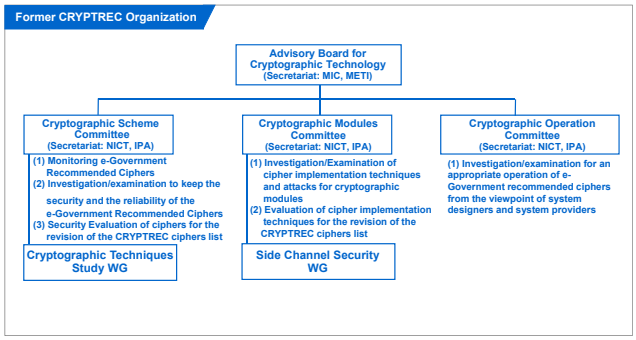


Fig. 1 Former CRYPTREC organization chart (from fiscal 2009 to fiscal 2012)

*1 CRYPTEC's activities during the 2nd Medium-term Plan (from fiscal 2006 to fiscal 2010) mainly handled by the Security Fundamental Laboratory were described in [1][4]–[9].

*2 The Information-technology Promotion Agency, Japan was mainly in charge of this work.

*3 It had a tentative name until before the fiscal 2012 amendment, but at the time of the fiscal 2012 amendment, it was formally named the "CRYPTREC Ciphers List."

CRYPTREC Ciphers List for use in e-Government systems, etc., from the viewpoints of IT system designers and operators.

2.2 Organization from Fiscal 2013 to Fiscal 2015

After the amendment of the e-Government Recommended Ciphers List, it was reorganized in fiscal 2013 as shown in Fig. 2. The activities of the Cryptographic Technology Evaluation Committee mainly handled by the Security Fundamentals Laboratory are described below.

Cryptographic Technology Evaluation Committee

This committee was established in fiscal 2013. It took over the activities which were handled by the Cryptographic Scheme Committee from fiscal 2009 to fiscal 2012, and part of the activities of the Cryptographic Module Committee. Specifically, it surveys and studies the matters described below in (1) to (3).

(1) Monitors and evaluates the security and implementations of cryptographic technology
(2) Surveys new-generation cryptography (lightweight cryptography, post-quantum cryptography, etc.)
(3) Surveys secure methods of using cryptographic technology (maintenance of technical guidelines, academic surveys and publications on security, etc.)

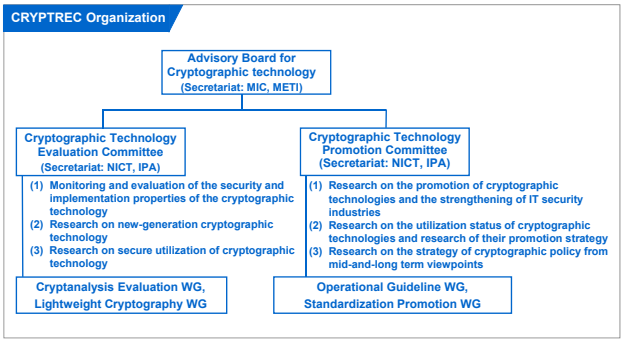


Fig. 2 CRYPTREC organization chart (from fiscal 2013 to fiscal 2015)

Table 1 List of dates for committee meetings held during 3rd Medium- to Long-Term Plan (1)

	Fiscal 2011		Fiscal 2012	
Cryptographic Scheme Committee	First	August 5, 2011	First	June 8, 2012
	Second	February 24, 2012	Second	July 24, 2012
	Third (Joint)	March 9, 2012	Third	October 9, 2012
			Fourth	March 5, 2013
			Fifth (Joint)	March 26, 2013
Cryptanalysis Evaluation Working Group (List Guide)	First	November 14, 2011	First	August 29, 2012
	Second	January 24, 2012	Second	December 20, 2012
	Third (Joint)	March 9, 2012	Third	February 25, 2013
			Fourth (Joint)	March 26, 2013
Cryptanalysis Evaluation Working Group (Computer Performance Evaluation)	First	October 6, 2011	First	December 21, 2012
	Second	December 21, 2011	Second	February 22, 2013
	Third (Joint)	March 9, 2012	Third (Joint)	March 26, 2013
Cryptographic Module Committee	First	September 12, 2011	First	July 5, 2012
	Second	December 19, 2011	Second	September 4, 2012
	Third	February 13, 2012	Third	October 9, 2012
	Fourth (Joint)	March 9, 2012	Fourth	March 14, 2013
			Fifth (Joint)	March 26, 2013
Side Channel Security Working Group	First	December 19, 2011	First	July 5, 2012
	Second	February 13, 2012	Second	March 14, 2013
	Third (Joint)	March 9, 2012	Third (Joint)	March 26, 2013
Cryptographic Operation Committee	First	September 21, 2011	First	June 8, 2012
	Second	November 18, 2011	Second	July 25, 2012
	Third	January 27, 2012	Third	October 4, 2012
	Fourth	February 24, 2012	Fourth	March 1, 2013
	Fifth (Joint)	March 9, 2012	Fifth (Joint)	March 26, 2013
			*Usage Survey Report Meeting	September 24, 2012
			*Joint Committee (Committee Chairs Meeting)	November 15, 2012

Cryptographic Technology Promotion Committee

This committee was established in fiscal 2013. It took over the activities that were done in the Cryptographic Operation Committee from fiscal 2009 to fiscal 2012, and part of the activities done in the Cryptographic Module Committee. Specifically, it surveys and studies the matters described below in (1) to (3) (fiscal 2013 and fiscal 2014).

(1) Studies to support wider use of cryptography, and strengthen the competitiveness of the security industry
(2) Surveys the situation of cryptographic technology use, studies necessary countermeasures, etc.
(3) Studies initiatives in cryptography policy, from medium and long term perspectives

Also, since fiscal 2015, aiming to contribute to the security of IT systems overall, it started an initiative for surveys and studies for maintenance and creating operations management.

2.3 Status of committee meetings held

Tables 1 (1) and (2) show the dates on which each meeting was held for committees etc. from fiscal 2011 to fiscal 2015.

3 Amendment of e-Government Recommended Ciphers List (in the 3rd Medium- to Long-term Plan)

During the 2nd Medium term Plan period, CRYPTEC mainly did the following:

(1) The draft outline for the revision of e-Government Recommended Ciphers List[*4]
(2) Cryptographic techniques submissions for the revision of e-Government Recommended Ciphers List (fiscal 2009)
(3) First security evaluations

Activities in the 3rd Medium- to Long-term Plan are described below.

3.1 Second security evaluations

In the second evaluations, we continued an overall evaluation of submitted cryptographic technologies that passed through the first evaluations, and reevaluated 128-Bit block ciphers etc. included in the former e-Government Recommended Ciphers List.[*5]

*4 We took the opportunity of creating the CRYPTREC Ciphers List this time to use the word "amendment" instead of "revision."
*5 In a narrow sense, it refers to the former evaluation only.

Table 1 List of dates for committee meetings held during 3rd Medium- to Long-Term Plan (2)

	Fiscal 2013		Fiscal 2014		Fiscal 2015	
Cryptographic Technology Evaluation Committee	First	July 29, 2013	First	August 4, 2014	First	18-Nov-15
	Second	December 13, 2013	Second	December 25, 2014	Second	8-Mar-16
	Third	March 6, 2014	Third	March 2, 2015		
			Fourth (Joint)	March 20, 2015		
Cryptanalysis Evaluation Working Group	First	September 3, 2013	First	September 2, 2014	First	22-Jan-16
	Second	February 20, 2014	Second	February 17, 204	Second	3-Mar-16
			Third (Joint)	March 20, 2015		
Lightweight Cryptography Working Group	First	September 17, 2013	First	August 29, 2014	First	20-Oct-15
	Second	December 26, 2013	Second	November 12, 2014	Second	24-Dec-15
	Third	February 20, 2014	Third	February 2, 2015	Third	9-Feb-16
			Fourth (Joint)	March 20, 2015		
Cryptographic Technology Promotion Committee	First	September 11, 2013	First	October 30, 2014	First	2-Mar-16
	Second	December 13, 2013	Second	January 26, 2015		
	Third	March 19, 2014	Third	March 10, 2015		
			Fourth (Joint)	March 20, 2015		
Operational Guideline Working Group	First	October 10, 2013	First	October 17, 2014		
	Second	December 4, 2013	Second	December 16, 2014		
	Third	March 12, 2014	Third	February 25, 2015		
			Fourth (Joint)	March 20, 2015		
Standardization Promotion Working Group	First	February 10, 2014	First	October 15, 2014		
	Second	February 10, 2014	Second	December 11, 2014		
			Third	February 23, 2015		
			Fourth (Joint)	March 20, 2015		

Submitted cryptographic technologies were evaluated for the performance of software and hardware. In the software performance, we evaluated by measuring the amount of memory used and initialization time in addition to processing speed. Also, for the hardware performance, we evaluated by measuring critical path delays, throughput, program size, etc., and to verify the feasibility of countermeasures against side channel attacks, we compared performances of the implementations with/without countermeasures, and evaluated the cost and the effectiveness of each against attacks. The Cryptographic Module Committee was put in charge of these performance evaluations of software and hardware. For details, see the CRYPTREC Report 2011 (Cryptographic Module Committee Report) [2] and CRYPTREC Report 2012 (Cryptographic Module Committee Report) [3].

3.1.1. Reevaluation of Cryptographic Technologies Included in the Former e-Government Recommended Ciphers List

In fiscal 2011, we evaluated the security of the key schedule for 128-bit block ciphers included in the former e-Government Recommended Ciphers List, and aiming to evaluate the security of related key attacks, we evaluated the upper bound of the differential characteristic probability of the key schedule. We also evaluated security for 192/256-bit keys, and in order to roughly estimate the complexity of 192/256-bit keys until related key attacks, we evaluated the upper bound of the differential/linear characteristic probabilities. In our evaluations, no flaws that could be realistic threats were found.

In fiscal 2012, for 128-bit block ciphers (submitted cryptographic technology CLEFIA, and former e-Government Recommended Ciphers AES, CIPHERUNICORN-A, Camellia, Hierocrypt-3, SC2000), we evaluated related key attacks and meet-in-the-middle attacks (including biclique attacks). In our evaluations, no flaws that could be realistic threats were found.

We evaluated the security of the stream cipher 128-bit RC4 in using SSL3.0 /TLS1.0 or higher, and in broadcast settings (like in cases using multiple different keys to encrypt the same plaintext), attacks that derive all bytes of the plaintext were reported, and we considered that they could be a realistic threat. For details, see the CRYPTEC Report 2011 (Cryptographic Scheme Committee Report) [4] and the CRYPTEC Report 2012 (Cryptographic Scheme Committee Report) [5].

3.2 The framework of selection rules

There was a need to evaluate the cryptographic technologies, based on the "Draft e-Government Recommended

Table 2 The selection criteria

Selection criteria concepts	Use the e-Government Recommended Ciphers List as a means of international standardization and commercialization promotion	
	While considering the outlook for "Security," "Current ease of procurement (utilization achievement in the real world market)" and "Future ease of procurement (utilization achievement in the real world market)," limit the number of items in the e-Government Recommended Ciphers List, and maximize consideration of "Other non-technical requirements" (how to encourage wider use of the proposed ciphers)	
	Consider the increasing trend that ciphers other than U.S. government standardized ciphers are excluded from international standardizations, specifications, and commercialization. Clarify the Japanese government's support for proposed ciphers.	
Selection criteria	(i) Select ciphers which already have sufficiently great current ease of procurement (utilization achievement in the real world market), sufficient security margin in the future, and that can also be expected to be used stably in the future.	
	(ii) Select ciphers for which the current ease of procurement (utilization achievement in the real world market) cannot be said to be sufficiently great, but that satisfy the following three conditions.	Evaluated as similar to those having the greatest security among the ciphers selected in (i), or greater.
		There are grounds to expect that supporting wider use in the future will have effects for international standardization and commercialization promotion.
		There are grounds to expect that supporting wider use in the future will sufficiently boost future ease of procurement (utilization achievement in the real world market).

Source: Advisory Board for Cryptographic Technology 2011 Report [6]

Ciphers Selection Criteria" [6] approved in the fiscal 2012 Cryptographic Scheme Committee, and in the fiscal 2011 Advisory Board for Cryptographic Technology. The matters studied in the Cryptographic Scheme Committee are explained in the subsection below, but before that, we give an overview of only the framework for selecting ciphers. For details on discussions in the Cryptographic Scheme Committee, see the CRYPTREC Report 2011 (Cryptographic Operation Committee Activities Report) [7] and the CRYPTREC Report 2012 (Cryptographic Operation Committee Activities Report) [8]. For details on discussions in the Advisory Board for Cryptographic Technology, see the Advisory Board for Cryptographic Technology Fiscal 2012 Report [9].

Based on the Fiscal 2011 Cryptographic Operation Committee Activities Report [7], the fiscal 2011 Advisory Board for Cryptographic Technology discussed draft criteria for selecting the next period's e-Government Recommended Ciphers. This resulted in the understanding that the next period's e-Government Recommended Ciphers will be selected according to the following concepts (Table 2). Based on these selection criteria, it was decided to select them by the method below (Fig. 3).

- The ciphers that could be selected by (i) are those judged as "Current utilization achievement in the real world market is sufficient" in Evaluation A (those that pass through selection route ①).
- The ciphers that could be selected by (ii) are those judged as "Current utilization achievement in the real world market cannot be said to be sufficient by Evaluation B, but that have high possibility of utilization promotion in the future" (those that pass through selection routes ② and ③).

3.2.1 Basic Policy

In the framework of approved selection rules, the Cryptographic Scheme Committee was required to study the following three items (blue arrows in Fig. 3).

1) "Security Evaluation"

For the ciphers to be evaluated, evaluate whether there are security issues for use in e-Government, and judge whether to put in the Candidate Recommended Ciphers List or exclude from the list.

2) "Evaluation B"

For the ciphers judged in "Evaluation A" to have insufficient utilization achievement in the real world market, judge "whether there are technical advantages to a degree that the market recognizes" regarding "security," as one item for judging whether there is high possibility of usage promotion in the future.

3) "Comprehensive Evaluation"

This evaluation was set up to narrow down the list further. Points are given to two "Technical as-

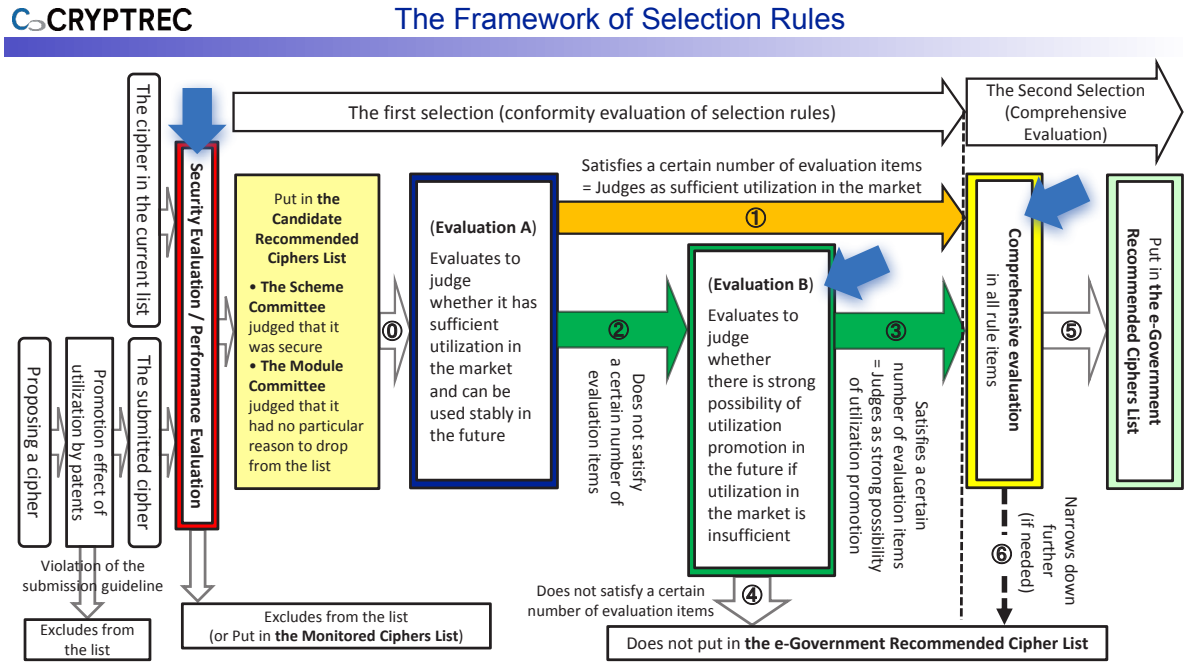


Fig. 3 The framework of selection rules
Circled numbers ⓪ to ⑥ in this diagram refer to selection steps.

Table 3 Selection policy on the security

①Selection policy for cryptographic technologies included in the list (fiscal 2002 version)	(a)Because of monitoring results, etc., security evaluations when the list (fiscal 2002 version) was developed are judged to be currently valid. However, if new attack methods, etc. are proposed, it is judged that there are also no security issues against them.
	(b)If comments on security are attached, it is judged that there are no security issues based on consideration whether that content is also currently valid.
	(c)If (a) and (b) are not satisfied, then it is put in the Monitored Ciphers List, in principle.
②Selection policy for fiscal 2009 submitted cryptographic technologies	(a)There should be no problems regarding security evaluations (if evaluations occurred this fiscal year, they are also taken into consideration).
	(b)If (a) is not satisfied, then it is left out of the next period's list.
③Selection policy for cryptographic technologies selected in secretariat	(a)There should be no problems regarding security evaluations (if evaluations re occurred this fiscal year, they are also taken into consideration).
	(b)If (a) is not satisfied, then it is left out of the next period's list, in principle.

Table 4 Evaluation policy and evaluation items for "Technical Appeal Points"

Evaluation policy for "Technical Appeal Points"	• Compare to other cryptographic algorithms in the same category of ciphers, and for any of the security related evaluation items in the scope specified by the secretariat, decide whether there are technically excellent points. If evaluation items outside the scope specified by the secretariat are included in inquiry results from the submitter, then they shall be approved if approved by the Cryptographic Scheme Committee.
	• In the case of submitted cryptographic technology, send inquiries to the submitter about them. In other cases, the secretariat shall investigate them.
	• If the Cryptographic Scheme Committee recognized that the content is valid, then it is decided there are "Technical Appeal Points."
Evaluation items for Technical Appeal Points	• Existence of certifiable security and ease of security evaluation
	• Validity of assumptions in provable security
	• Reduction efficiency of provable security
	• Existence of efficient attack by exhaustive key search, etc.
	• Security margin (longest attackable number of rounds at current time)
	• Existence of restrictions on security related usage
	• International conferences and journals where the paper on which the cipher was proposed was accepted

pects" evaluation items: "Security advantages in accordance with specifications" and "Advantage by number of papers." This was not enforced this time, because it was judged unnecessary in the Advisory Board for Cryptographic Technology.

3.2.2 "Security Evaluation" Judgment Method

There are three cryptographic technologies to be studied: ① Cryptographic technologies included in the list (fiscal 2002 version), ② Fiscal 2009 submitted cryptographic technologies (including 3 cipher categories: 128-bit block ciphers / stream ciphers / message authentication codes), ③ Secretariat selected cryptographic technologies (message authentication codes / modes of operation / entity authentication). The Cryptographic Scheme Committee decided security related judgment policy as described in ① to ③ below (Table 3).

3.2.3 Evaluation Items and Points Allocation for "Evaluation B" and "Comprehensive Evaluation"

(1) "Evaluation B" related evaluation items

In "Evaluation B," "whether there are technical advantages to a degree that the market recognizes" (hereinafter, "Technical Appeal Points") is one item set up to judge whether there is a large possibility of utilization promotion in the future.[*6] The Cryptographic Scheme Committee made evaluation policies and evaluation items as "security" related Technical Appeal Points, as shown in Table 4.

(2) "Comprehensive Evaluation" related evaluation items

*6 Technical Appeal Points have 2 viewpoints: The Cryptographic Scheme Committee evaluates security, and the Cryptographic Module Committee evaluates software/hardware performance. If the cryptographic technology under evaluation is judged to have advantage in terms of either or both of them, then it is judged to have Technical Appeal Points.

Evaluation policy for "Comprehensive Evaluation" evaluation item "Security advantages in accordance with specifications" was approved as shown in Table 5. Also, evaluation policy for "Comprehensive Evaluation" evaluation item "Advantage by number of papers" was approved as shown in Table 6. As a method for converting the number of citations into points, the number of citations from the time of proposal to the end of August 2012 itself is used as the number of points, with the allocation points (20 points) as the upper bound.

(3) Points allocation for "Comprehensive Evaluation"

When allocating points for "Security advantages in accordance with specifications" and "Advantage by number of papers," "Advantage by number of papers" is treated equally to each evaluation item for "Security

Table 5 Evaluation policy for "Security advantages in accordance with specifications"

Evaluation policy for "Security advantages in accordance with specifications"	• Each category of ciphers has the same number of evaluation items.		
	• Each evaluation item has the same ratio of points.		
	• Evaluation items of each category of ciphers are as written to right (5 evaluation items)	(a) Public key ciphers	(1) Existence of provable security
			(2) Validity of assumptions of provable security
			(3) Degree of reduction efficiency
			(4) Existence of utilization restrictions
			(5) Acceptance of the paper for the proposed cipher by a peer-reviewed international conference or journal
		(b) Symmetric key ciphers (64-bit & 128-bit block ciphers, stream ciphers)	(1) Existence of provable security or Ease of security evaluation.
			(2) Existence of more efficient attacks than brute-force attack
			(3) Security margin (longest attackable number of rounds / full round)
			(4) Existence of utilization restrictions
			(5) Acceptance of the paper for the proposed cipher by a peer-reviewed international conference or journal
		(c) Hash function	(1) Hash length (256 bit or longer)
			(2) Security margin for collision resistance (longest attackable number of rounds / full round)
			(3) Security margin for second pre-image resistance (longest attackable number of rounds / full round)
			(4) Security margin for pre-image resistance (longest attackable number of rounds / full round)
			(5) Existence of utilization restrictions
		(d) Message authentication codes	(1) Existence provable security
			(2) Validity of assumptions for provable security
			(3) Degree of reduction efficiency
			(4) Existence of utilization restrictions
			(5) Acceptance of the paper for the proposed ciphers by a peer-reviewed international conference or journal
		(e) Modes of operation	(1) Existence of provable security
			(2) Validity of assumptions for provable security
			(3) Degree of reduction efficiency
			(4) Existence of utilization restrictions
			(5) Acceptance of the paper for the proposed cipher by a peer-reviewed international conference or journal
		(f) Entity authentication	(1) Existence of provable security?
			(2) Validity of assumptions for provable security
			(3) Degree of reduction efficiency
			(4) Existence of utilization restrictions
			(5) Acceptance of the paper for the proposed ciphers by a peer-reviewed international conference or journal?

Table 6 Evaluation policy for "Advantage by number of papers"

Evaluation policy for "Advantage by number of papers"	Judge whether literature that proposed the cipher has many or few citations.
	Only evaluate papers on security evaluation of the cipher being surveyed. In order to limit to papers on security evaluation, for ciphers with many citations, use sampling to estimate the number of citations.
	The survey scope for citing papers is journals and peer-reviewed international conferences with papers published in Springer LNCS, IEEE or ACM. For survey places, use search websites (example: Google Scholar, http://scholar.google.co.jp/) or existing academic databases.
	If there are multiple candidates for cited papers which proposed the cipher, then survey based on three major papers. Also, exclude duplicates as much as possible.
	Do not adjust due to variations in points between cipher categories.

Table 7 Points allocation for "Comprehensive Evaluation"

Points allocation for "Comprehensive Evaluation"	Security advantages of specifications (5 items in each category of ciphers)	100
	Advantage by number of papers	20

Table 8 "Security Evaluation" judgment results[*7]

Judgment result of security evaluation	Category of ciphers	Name of cipher
Cryptographic technology decided as Recommended Candidate Cipher	Signature	DSA, ECDSA, RSA-PSS, RSASSA-PKCS1 -v1 _5
	Confidentiality	RSA-OAEP
	Key exchange	DH, ECDH, PSEC-KEM (with note)
	64-bit block cipher (with note)	CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, 3 -key Triple DES (with note)
	128-bit block cipher	AES, Camellia, CIPHERUNICORN-A, CLEFIA, Hierocrypt-3, SC2000
	Stream cipher	Enocoro-128 v2, KCipher-2, MUGI, MULTI-S01 (with note)
	Hash function	SHA-256, SHA-384, SHA-512
	Modes of operation	CBC, CFB, CTR, OFB, CCM, GCM (with note)
	Message authentication code	CMAC, HMAC, PC-MAC-AES
	Entity code	ISO/IEC 9798 -2, ISO/IEC 9798 -3, ISO/IEC 9798 -4
Cryptographic technology decided as Monitored Cipher	Confidentiality	RSAES-PKCS1 -v1 _5
	Stream cipher	128 -bit RC4 (with note)
	Hash function	RIPEMD-160, SHA-1
	Message authentication code	CBC-MAC (with note)

advantages in accordance with specifications," and if the total number of evaluation items for "Security advantages in accordance with specifications" is N, then that relative ratio is determined to be N:1. Based on approved points allocation, the allocation points of "Comprehensive Evaluation" evaluation items "Security advantages in accordance with specifications" and "Advantage by number of papers" are as shown in Table 7.

3.3 "Security Evaluation" judgment result and the CRYPTEC Ciphers List

In the approved framework of selection rules, before applying them to Evaluation A, Evaluation B and Comprehensive Evaluation, the list (fiscal 2002), newly submitted ciphers and secretariat selected ciphers must be classified into the Candidate Recommended Ciphers or the Monitored Ciphers. The Cryptographic Scheme Committee decided whether they are the Candidate Recommended Ciphers, as shown in Table 8.

After that, the draft of "The List of Ciphers that Should Be Referred to in the Procurement for the e-Government System (CRYPTREC Ciphers List)," which was decided on the basis of the evaluation results by 3 committees (Cryptographic Scheme Committee, Cryptographic Module

*7 Later, for RSA and SHA-1, a note was added regarding "Migration Guidelines for SHA-1 and RSA1024 Cryptographic Algorithms Used in Information Systems of Government Agencies" (In April 2008 determined by Information Security Policy Council, and in October 2012 Revised by Information Security Policy Council).

Table 9 CRYPTREC Ciphers List (March 1, 2013, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry)
(1) e-Government Recommended Ciphers List (2) Candidate Recommended Ciphers List (3) Monitored Ciphers List

e-Government Recommended Ciphers List

The list of recommended cryptographic techniques[1], for which the Advisory Board for Cryptographic Technology[2] and the related committees (henceforth "CRYPTREC") confirmed the security, the implementation efficiency, and the sufficient market deployment so far or the expected spread in the future.

Category of technique		Name
Public-key cryptographic techniques	Signature	DSA
		ECDSA
		RSA-PSS(Note 1)
		RSASSA-PKCS-v1_5(Note 1)
	Confidentiality	RSA-OAEP(Note 1)
	Key agreement	DS
		ECDH
Symmetric-key cryptographic techniques	64-bit block ciphers(Note 2)	3-key Triple DES(Note 3)
	128-bit block ciphers	AES
		Camellia
	Stream ciphers	KCipher-2
Hash functions		SHA-256
		SHA-384
		SHA-512
Modes of operation	Confidentiality modes	CBC
		CFB
		CTR
		OFB
	Authenticated encryption modes	CCM
		GCM(Note 4)
Message authentication codes		CMAC
		HMAC
Entity authentication protocols		ISO/IEC 9798-2
		ISO/IEC 9798-3

(Note 1) These cryptographic techniques should be used based on "Migration Plan of Cryptographic Algorithm SHA-1 and RSA1024 in the Information Systems of Government Agencies" (Decision at the Information Security Policy Council in April, 2008; Revision at Information Security Measures Promotion Council in October, 2012.) http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf (March 1, 2013; in Japanese)

(Note 2) If a block cipher with a longer block length can be used, it is preferable to choose a 128-bit block cipher.

(Note 3) The 3-key Triple DES is permitted to be used for the time being under the following conditions:

1)! It is specified as NIST SP 800-67.

2)! It maintains a position as a de facto standard.

(Note 4) The recommended size of an initialization vector is 96 bits.

[1] The modes of operation, the message authentication codes and the entity authentication protocols are supposed to be used in combination with a cryptographic technique in other categories, which is included in the CRYPTREC Ciphers List.

[2] The Advisory Board for Cryptographic Technology was set up in order to contribute to the study of measures in the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI), by gathering experts in the related fields under the names of the Director-General for ICT Strategic Policy Planning of MIC and the Director-General of Commerce and Information Policy Bureau of METI, from a viewpoint of promotion of the information security measures by the spread of cryptographic techniques.

Candidate Recommended Ciphers List

The list of cryptographic techniques[3], for which CRYPTREC confirmed the security and the implementation efficiency, and which have the possibility to be included in the e-Government Recommended Ciphers list hereafter.

Category of technique		Name
Public-key cryptographic techniques	Signature	NA
	Confidentiality	NA
	Key agreement	PSEC-KEM(Note 5)
Symmetric-key cryptographic techniques	64-bit block ciphers(Note 6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128-bit block ciphers	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	Stream ciphers	Enocoro-128v2
		MUGI
		MULTI-S01(Note 7)
Hash functions		NA
Modes of operation	Confidentiality modes	NA
	Authentication encryption modes	NA
Message authentication codes		PC-MAC-AES
Entity authentication protocols		ISO/IEC 9798-4

(Note 5) This is permitted to be used only in the KEM (Key Encapsulating Mechanism) - DEM (Data Encapsulating Mechanism) construction.

(Note 6) If a block cipher with a longer block length can be used, it is preferable to choose a 128-bit block cipher.

(Note 7) The plaintext size is restricted to a multiple of 64 bits.

[3] The modes of operation, the message authentication codes and the entity authentication protocols are supposed to be used in combination with a cryptographic technique in other categories, which is included in the CRYPTREC Ciphers List.

Monitored Ciphers List

The list of cryptographic techniques[4], which should not be recommended due to an increased risk of compromise etc., but are admitted for continuous use in order to achieve interoperability. The listed techniques are not recommended for any purposes other than to achieve interoperability.

Category of technique		Name
Public-key cryptographic techniques	Signature	NA
	Confidentiality	RSAES-PKCS1-v1_5(Note 8)(Note 9)
	Key agreement	NA
Symmetric-key cryptographic techniques	64-bit block ciphers	NA
	128-bit block ciphers	NA
	Stream ciphers	128-bit RC4(Note 10)
Hash functions		RIPEMD-160
		SHA-1(Note 8)
Modes of operation	Confidentiality modes	NA
	Authentication encryption modes	NA
Message authentication codes		CBC-MAC(Note 11)
Entity authentication protocols		NA

(Note 8) These cryptographic techniques should be used based on "Migration Plan of Cryptographic Algorithm SHA-1 and RSA1024 in the Information Systems of Government Agencies" (Decision at the Information Security Policy Council in April, 2008; Revision at Information Security Measures Promotion Council in October, 2012.) http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf (March 1, 2013; in Japanese)

(Note 9) The algorithm is permitted to be used for the time being because it is used in SSL 3.0/TLS 1.0, 1.1, 1.2.

(Note 10) Use of 128-bit RC4 should be limited to SSL 3.0/TLS (1.0 or later).

(Note 11) CBC-MAC is not secure for variable-length messages, so the message length should be fixed..

[4] The modes of operation, the message authentication codes and the entity authentication protocols are supposed to be used in combination with a cryptographic technique in other categories, which is included in the CRYPTREC Ciphers List.

Committee and Cryptographic Operation Committee), was approved by the Advisory Board for Cryptographic Technology, and it was decided to solicit public comments. Then the list was finally endorsed by the Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry on March 1, 2013 (Friday) (Table 9).

4 Cryptographic Technology Evaluation Committee activities

In fiscal 2013, its name was changed from "Cryptographic Scheme Committee" to "Cryptographic Technology Evaluation Committee." It now carries out technical studies focused on security evaluations of cryptographic technology:

(a) Surveys on new-generation cryptographic technology (lightweight cryptography, security parameters, pairing-based cryptography, post-quantum cryptography, etc.)

(b) Monitoring and evaluation of the security of cryptographic technology

(c) Surveys on the secure utilization of cryptographic technology (maintenance of technical guidelines, academic surveys on the security of cryptography and their publications, etc.)

The subsection below briefly explains its main activities.

4.1 Change of the reference for specifications

Regarding the DSA (from NIST FIPS 186-2 (+Change Notice) to NIST FIPS 186-4), extending of the sizes of finite fields and the length of the output of hash functions are judged as simple revisions such as parameter revisions, and the change of the reference for specifications was approved.

4.2 Study of replies to questions from the Cryptographic Technology Promotion Committee

Technical views were sought from the Cryptographic Technology Promotion Committee regarding perfect for-

ward secrecy and forward secrecy, so replies were given.

4.3 Issuance of Cryptographic Technology Guidelines

4.3.1 CRYPTREC Cryptographic Technology Guidelines (recent attacks on SSL/TLS)

In fiscal 2013, it provided an outline of techniques of recent attacks on SSL/TLS, and analyzed effects on IT systems. It created guidelines regarding attacks on SSL/TLS in recent years, concerning effects from the viewpoint of security in cipher suites.

4.3.2 CRYPTREC Cryptographic Technology Guideline (SHA-1)

For e-Government system procurers and e-Government system developers, this describes the information required when using the SHA-1 hash function put in the Monitored Ciphers List of the CRYPTREC Ciphers List. That is, it describes deprecated and approved usages of SHA-1 and reference information for SHA-1.

4.4 A changes to the note of 128-bit Key RC4

128-bit key RC4 was put in the Monitored Ciphers List. The note "128 -bit RC4 shall only be used in SSL (TLS 1.0 or higher)" was added. Considering reported vulnerabilities in recent years, the proposed change to this note was decided: "Continued use to maintain compatibility has been tolerated up to now, but it should not be used as much as possible in the future. Including the usage in SSL/TLS, promptly consider migrating to a cryptographic technology included in the e-Government Recommended Ciphers List."

4.5 Warning reports

If it is judged desirable to quickly publish outlines of attacks announced at international conferences etc., ranges of possible effects of attacks, and countermeasures, through activities monitoring security and implementation of cryptographic technology included in the CRYPTEC Ciphers List, a Warning Report about them will be issued. The Cryptographic Technology Evaluation Committee has issued the following Warning Reports in the past.

"Dual_EC_DRBG Pseudorandom Number Generator Algorithm" (Nov. 6, 2013) [10]

"Security of MISTY1 64-bit Block Cipher (July 16, 2015)" [11]

"Security of MISTY1 64-bit Block Cipher (August 12, 2015)" [12]

"Security of SHA-1 (December 18, 2015)" [13]

4.6 Handling of SHA-2 and SHA-3 hash functions

Addition of cryptographic technologies judged as expected to be used in e-Government systems, etc. was considered. Discussions in the Cryptographic Technology Evaluation Committee resulted in the decision to only use algorithms with 256-bit or longer hash lengths. The specific algorithms applied by this condition are as follows.

SHA-2: SHA-512 /256

SHA-3: SHA3 -256, SHA3 -384, SHA3 -512, SHAKE256

4.7 Cryptanalysis Evaluation Working Group

Security of public key cryptography depends on various mathematical problems, such as the difficulty of the factoring problem and difficulty of the discrete logarithm problem. Besides the difficulty of the factoring problem and difficulty of the discrete logarithm problem, this working group surveys the difficulty of mathematical problems that support "post-quantum cryptography" that is expected to remain secure even if large-scale quantum computers are available for use. For details, see the CRYPTREC Report 2013 (Cryptographic Technology Evaluation Committee Activities Report) [14], CRYPTREC Report 2014 (Cryptographic Technology Evaluation Committee Activities Report) [15], and CRYPTREC Report 2015 (Cryptographic Technology Evaluation Committee Activities Report) [16].

4.8 Lightweight Cryptography Working Group

This group surveys lightweight cryptography proposed until now (regarding security, performance, applications, etc.), with the aim that users can select and easily procure suitable methods for not only e-Government systems but also services that need lightweight cryptography. It also plans to issue "Cryptographic Technology Guidelines (Lightweight Cryptography)" that contributes to technical decisions when selecting and using lightweight cryptography, and aims to encourage future use. For details, see the CRYPTREC Report 2013 (Cryptographic Technology Evaluation Committee Activities Report) [14], CRYPTREC Report 2014 (Cryptographic Technology Evaluation Committee Activities Report) [15], and CRYPTREC Report 2015 (Cryptographic Technology Evaluation Committee Activities Report) [16].

5 Future issues

When developing the "Draft Outline for the revision of

the e-Government Recommended Ciphers List," the List Guide was intended to be positioned in the Ciphers List (refer to [1], Fig. 9). Initiatives like developing the List Guide that provide information on appropriate methods of using cryptographic technology to system operators and users are considered to be important, so in current CRYPTREC activities, the Cryptographic Technology Evaluation Committee and Cryptographic Technology Promotion Committee are continuing work on cryptographic technology guidelines and cryptographic operations guidelines. However, as far as the current CRYPTREC Ciphers List is concerned, one cannot see direct links between those guidelines and the list. We think that how to unify these initiatives with the list to carry them out in a form in accordance with the draft outline remains to be solved.

6 Conclusion

This paper described the activities of CRYPTEC from fiscal 2011 to fiscal 2015, mainly handled by the Security Fundamentals Laboratory. It also described evaluations done when amending the e-Government Recommended Ciphers List.

Acknowledgments

We take this opportunity to thank all those who participated in CRYPTREC activities until now, and those who cooperated in studying security evaluations and performance evaluations of cryptographic algorithms. We are especially grateful to Emeritus Professor of the University of Tokyo, Hideki Imai, who supported CRYTREC activities by serving for a long time as Chairman of committees such as the Cryptographic Technology Evaluation Committee until fiscal 2014.

References

1 Takashi Kurokawa and Sachiko Kanamori, "CRYPTREC Activities," Journal of the National Institute of Information and Communications Technology (Special Issue on Network Security), vol.58 nos.3/4, pp.249–265, September/December 2011.

2 Cryptographic Module Committee, "CRYPTREC Report 2011 (Report of the Cryptographic Module Committee)," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2012. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

3 Cryptographic Module Committee, "CRYPTREC Report 2012 (Report of the Cryptographic Module Committee)," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2013. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

4 Cryptographic Scheme Committee, "CRYPTREC Report 2011 (Report of the Cryptographic Scheme Committee)," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2012. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

5 Cryptographic Scheme Committee, "CRYPTREC Report 2012 (Report of the Cryptographic Scheme Committee)," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2013. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

6 Advisory Board for Cryptographic Technology, "Report of the Advisory Board for Cryptographic Technology in FY 2011,", Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry, March 2012. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

7 Cryptographic Operation Committee, "CRYPTREC Report 2011 (Report of the Cryptographic Operation Committee)," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2012. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

8 Cryptographic Operation Committee, "CRYPTREC Report 2012 (Report of the Cryptographic Operation Committee)," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2013. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

9 Advisory Board for Cryptographic Technology, "Report of the Advisory Board for Cryptographic Technology in FY 2012,", Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry, March 2013. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

10 Cryptographic Technology Evaluation Committee, "On Random Bit Generation Algorithm Dual_EC_DRBG," Cryptographic Technology Evaluation Committee, November 2013.
Available at http://www.cryptrec.go.jp/english/topics/cryptrec_20131106_dual_ec_drbg.html

11 Cryptographic Technology Evaluation Committee, "On the Security of 64-bit Block Cipher MISTY1," Cryptographic Technology Evaluation Committee, July 2015.
Available at http://www.cryptrec.go.jp/english/topics/cryptrec_20150716_misty1_cryptanalysis.html

12 Cryptographic Technology Evaluation Committee, "On the Security of 64-bit Block Cipher MISTY1 (Another new result)," Cryptographic Technology Evaluation Committee, August 2015.
Available at http://www.cryptrec.go.jp/english/topics/cryptrec_20150812_misty1_cryptanalysis.html

13 Cryptographic Technology Evaluation Committee, "On the Security of hash functions SHA-1," Cryptographic Technology Evaluation Committee, December 2015. (In Japanese)
Available at http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html

14 Cryptographic Technology Evaluation Committee, "CRYPTREC Report 2013 (Report of the Cryptographic Technology Evaluation Committee)," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2014. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

15 Cryptographic Technology Evaluation Committee, "CRYPTREC Report 2014 (Report of the Cryptographic Technology Evaluation Committee)," National Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2015. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

16 Cryptographic Technology Evaluation Committee, "CRYPTREC Report 2015 (Report of the Cryptographic Technology Evaluation Committee)," National

Institute of Information and Communications Technology and Information Promotion Agency, Japan, March 2016. (In Japanese)
Available at http://www.cryptrec.go.jp/report.html

Takashi KUROKAWA

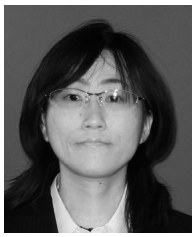
Technical Expert, Security Fundamentals Laboratory, Cybersecurity Research Institute
Security Evaluations of Cryptographic Technologies

Sachiko KANAMORI

Technical Expert, Security Fundamentals Laboratory, Cybersecurity Research Institute
Privacy

Ryo NOJIMA, Ph.D.

Senior Researcher, Security Fundamentals Laboratory, Cybersecurity Research Institute
Cryptography, Cryptographic Protocol



Miyako OHKUBO, Ph.D.

Senior Researcher, Security Fundamentals Laboratory, Cybersecurity Research Institute
Cryptography, Cryptographic Protocol

Shiho MORIAI, Ph.D.

Director of Security Fundamentals Laboratory, Cybersecurity Research Institute
Cryptography, Information Security