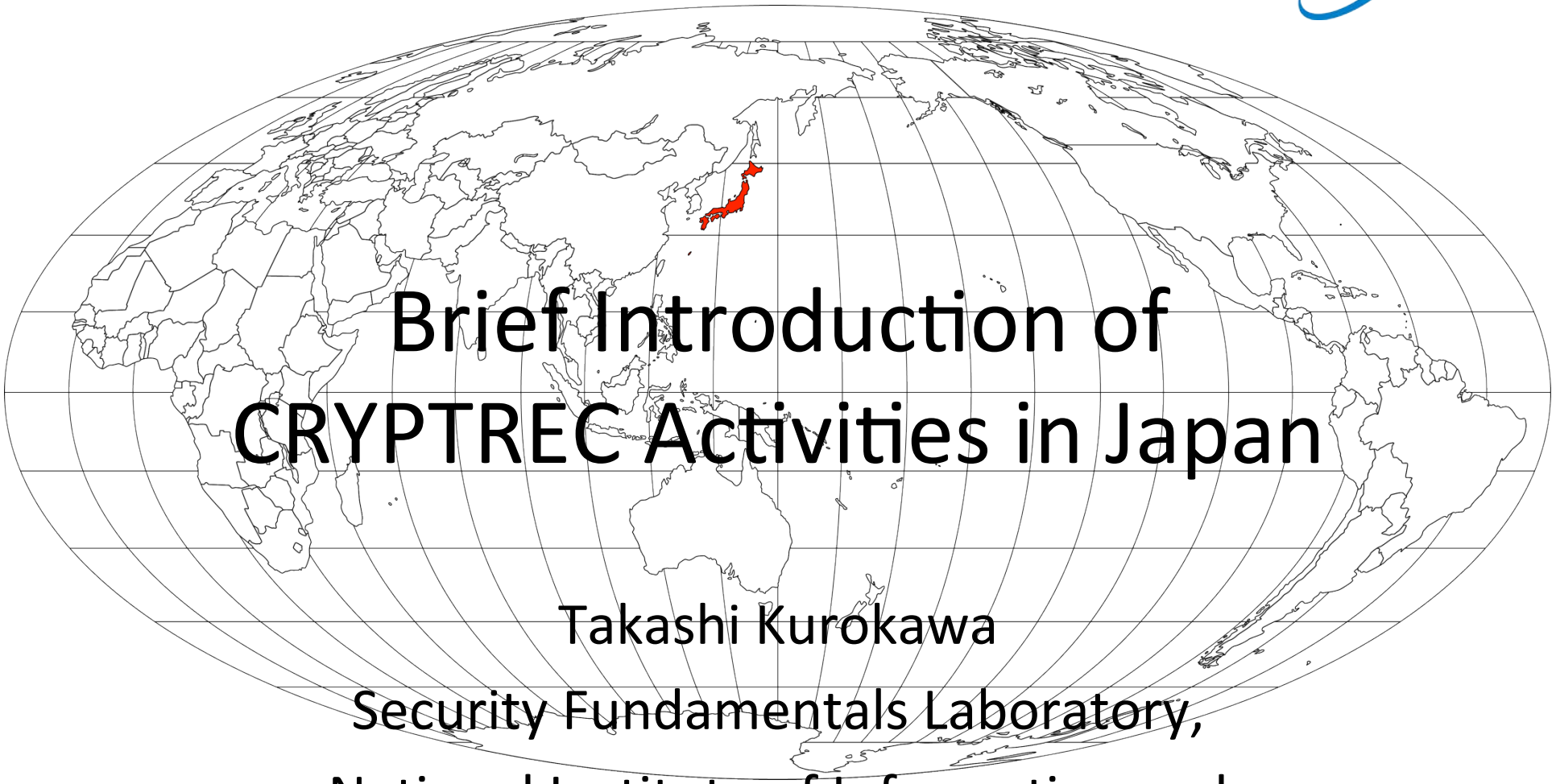


Brief Introduction of CRYPTREC Activities in Japan

Takashi Kurokawa
Security Fundamentals Laboratory,
National Institute of Information and Communications Technology

CRYPTREC

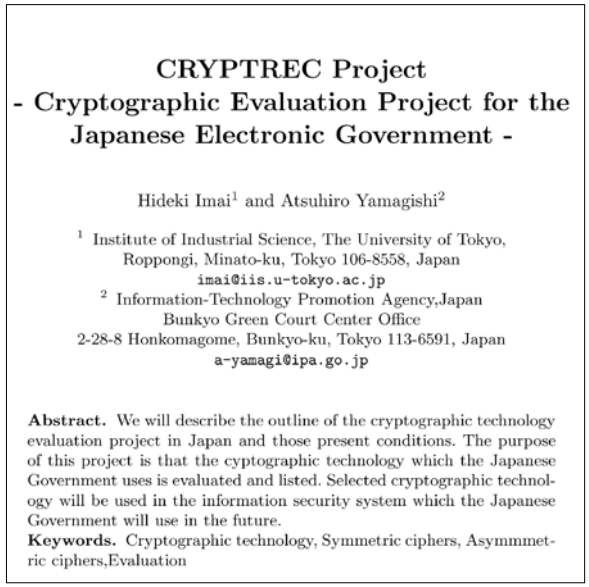
- About 12 years ago:
  - H. Imai and A. Yamagishi.

    Invited Lecture of

    ASIACRYPT 2000,

    Kyoto, JAPAN

    CRYPTREC Project - Cryptographic Evaluation Project for the Japanese Electronic Government –. Volume 1976 of LNCS, pp.399–400, 2000.



CRYPTREC Project
- Cryptographic Evaluation Project for the Japanese Electronic Government -

Hideki Imai[1] and Atsuhiro Yamagishi[2]

[1] Institute of Industrial Science, The University of Tokyo, Roppongi, Minato-ku, Tokyo 106-8558, Japan
imai@iis.u-tokyo.ac.jp
[2] Information-Technology Promotion Agency,Japan Bunkyo Green Court Center Office
2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591, Japan
a-yamagi@ipa.go.jp

Abstract. We will describe the outline of the cryptographic technology evaluation project in Japan and those present conditions. The purpose of this project is that the cyptographic technology which the Japanese Government uses is evaluated and listed. Selected cryptographic technology will be used in the information security system which the Japanese Government will use in the future.
Keywords. Cryptographic technology, Symmetric ciphers, Asymmmetric ciphers,Evaluation

CRYPTREC (cont.)

- CRYPTography Research and Evaluation Committees.
- Research project in Japan since 2000.
- Conducts security evaluations which can contribute to the realization of e-Government.
- Makes a list of secure cryptographic techniques which are examined closely by a lot of experts (domestic and international).
- URL `http://www.cryptrec.go.jp/`

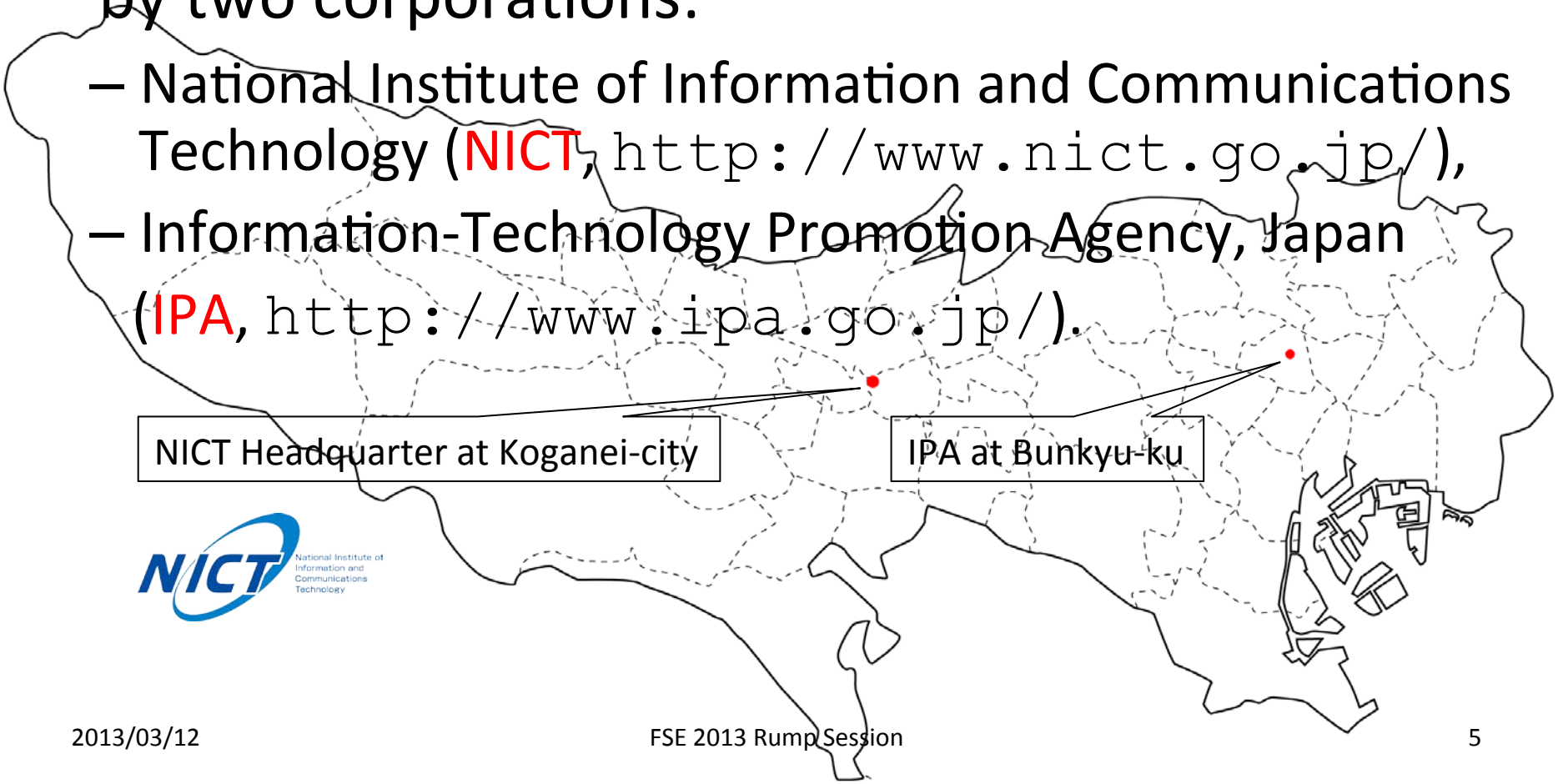
Organization

- Divided into two parts:

1. An advisory board is run by two ministries:
   - The Ministry of Internal affairs and Communication (MIC, http://www.soumu.go.jp),
   - the Ministry of Economy, Trade and Industry (METI, http://www.meti.go.jp/).

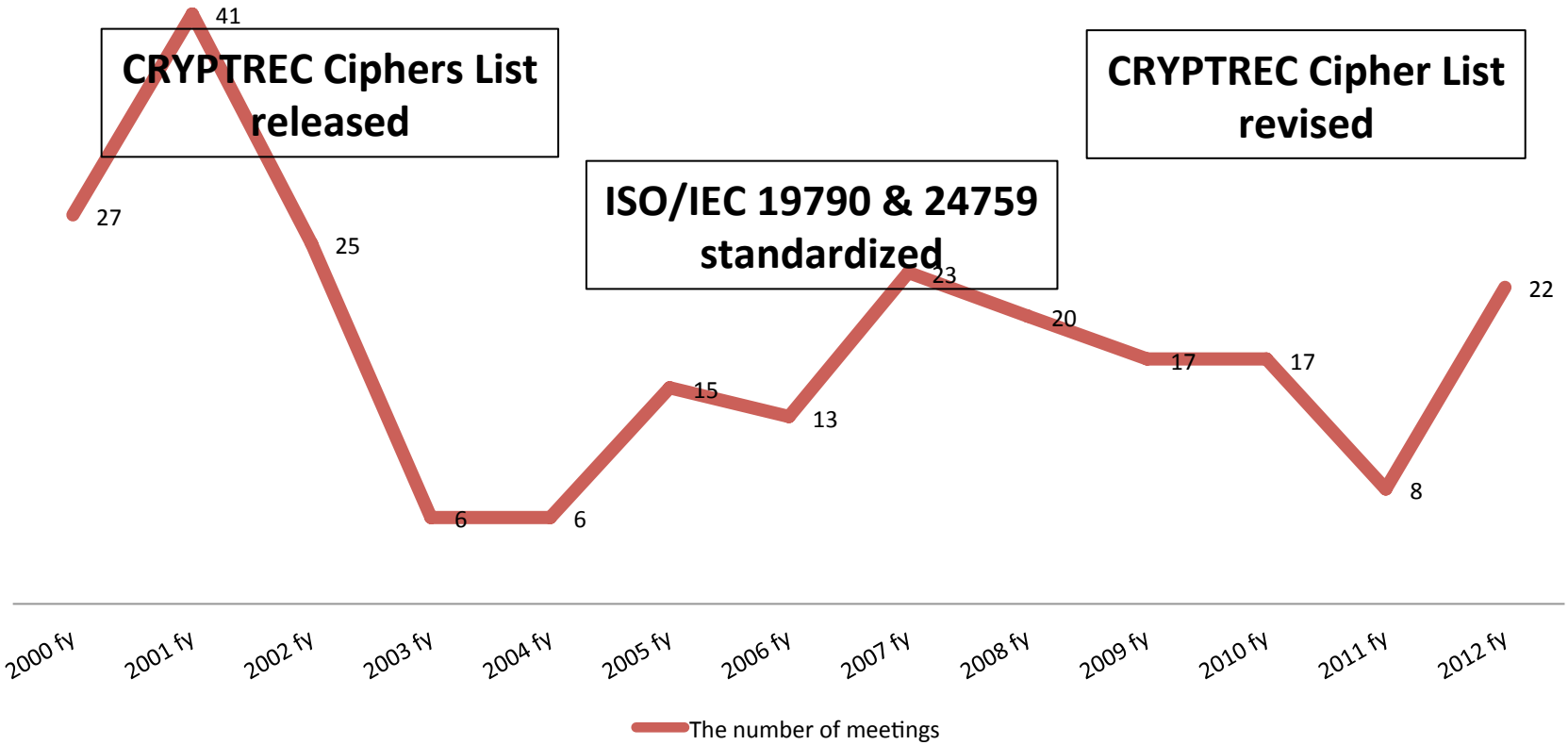
Organization (cont.)

2. Several committees and working groups are run by two corporations:
   - National Institute of Information and Communications Technology (NICT, `http://www.nict.go.jp/`),
   - Information-Technology Promotion Agency, Japan (IPA, `http://www.ipa.go.jp/`).



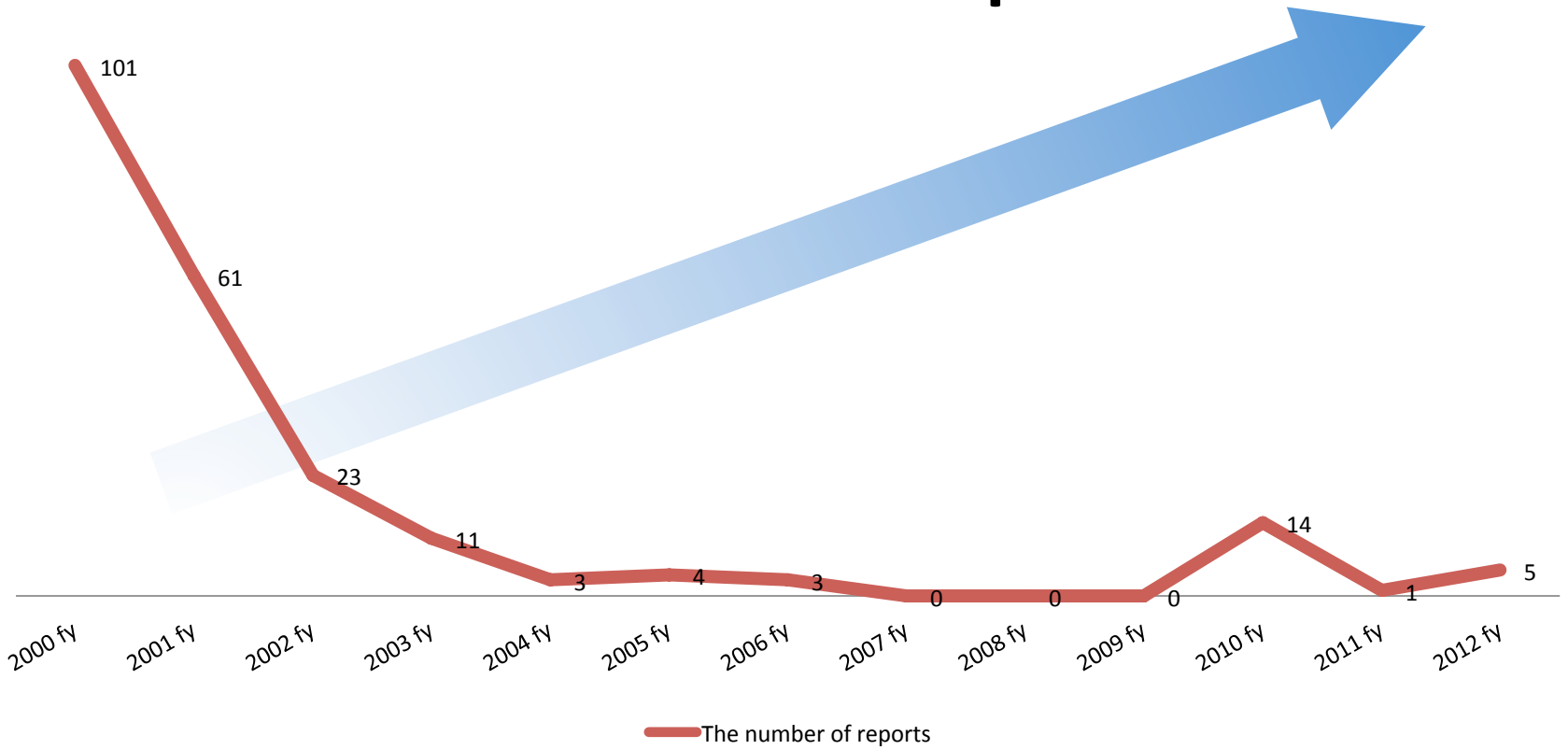
Statistics

The number of meetings



Statistics (cont.)

The number of reports



e-Government Recommended Ciphers List (FY 2002 Edition)

Category of technique		Name
Public-key cryptographic techniques	Signature	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	Confidentiality	RSA-OAEP
		RSAES-PKCS1-v1_5 (Note 1)
	Key agreement	DH
		ECDH
		PSEC-KEM (Note 2)
Symmetric-key cryptographic techniques	64-bit block ciphers (Note 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES (Note 4)
	128-bit block ciphers	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	Stream ciphers	MUGI
		MULTI-S01
		128-bit RC4 (Note 5)
Other	Hash functions	RIPEMD-160 (Note 6)
		SHA-1 (Note 6)
		SHA-256
		SHA-384
		SHA-512
		PRNG based on SHA-1 in ANSI X9.42-2001 Annex
		186-2 (+ change notice 1) revised Appendix 3.1

http://www.cryptrec.go.jp/english/list.html

CRYPTREC Ciphers List (FY 2012 Edition) NEW!

- Revised and released this March!
- Divided into three parts:
  - e-Government Recommended Ciphers List
  - Candidate Recommended Ciphers List NEW!
    - Expect to be popular in the near future!
  - Monitored Ciphers List NEW!
    - Backward compatibility or deprecated
- Three standard categories are added.
- Website in English will be updated soon.

e-Government Recommended Ciphers List (FY 2012 Edition) NEW!

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号	3-key Triple DES
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2 NEW!!
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード NEW!	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM
メッセージ認証コード NEW!		CMAC
		HMAC NEW!!
エンティティ認証 NEW!		ISO/IEC 9798-2 NEW!!
		ISO/IEC 9798-3

(In Japanese)

Candidate Recommended Ciphers List (FY 2012 Edition) NEW!

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM
共通鍵暗号	64 ビットブロック暗号	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128 ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA NEW!!
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2 NEW!!
		MUGI
		MULTI-S01
ハッシュ関数		該当なし
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES NEW!!
エンティティ認証		ISO/IEC 9798-4 NEW!!

(In Japanese)

Monitored Ciphers List

NEW!

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5
	鍵共有	該当なし
共通鍵暗号	64 ビットブロック暗号	該当なし
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4
ハッシュ関数		RIPEMD-160
		SHA-1
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		CBC-MAC NEW!!
エンティティ認証		該当なし

(In Japanese)

Last but not least

- We would like to take this opportunity to thank all of the reviewers who have helped make our lists.