CRYPTREC2001
Report on Present State of Symmetric-Key Cipher Evaluations

January 28, 2002

Toshinobu Kaneko

Chair, Symmetric-Key Cryptography Subcommittee

Professor, Science University of Tokyo

Ciphers to be evaluated

- **Submitted cipher categories**
  - Ciphers submitted in FY2000
  - Other ciphers requiring evaluation
  - Ciphers newly submitted in FY2001 → Part II

  } Part I

- **Cryptographic technique categories**
  - Symmetric-key ciphers (64- and 128-bit block ciphers)
  - Symmetric-key ciphers (stream ciphers)
  - Hash functions
  - Pseudo-random number generators

Symmetric-Key Cryptography Subcommittee

Kiyomichi Araki	**(Tokyo Institute of Technology)**
Toshinobu Kaneko	**(Science University of Tokyo)**
Shinichi Kawamura	**(Toshiba Corporation)**
Masayuki Kanda	**(Nippon Telegraph and Telephone Corporation)**
Tohru Kohda	**(Kyushu University)**
Kazukuni Kobara	**(University of Tokyo)**
Kouichi Sakurai	**(Kyushu University)**
Takeshi Shimoyama	**(Fujitsu Laboratories, Ltd.)**
Kazuo Takaragi	**(Hitachi, Ltd.)**
Makoto Tatebayashi	**(Matsushita Electric Industrial Co., Ltd.)**
Yukiyasu Tsunoo	**(NEC Corporation)**
Toshio Tokita	**(Mitsubishi Electric Corporation)**
Masakatu Morii	**(University of Tokushima)**

I. Evaluations in current fiscal year

- **Ciphers submitted in FY2000 (S2000)**
  - Judgments based on CRYPTREC2000 report
  - Verification of cipher submitter's intention to continue submission

  → **Monitored ciphers:**
    - Full evaluations completed with CRYPTREC Report 2000
    - E-government cipher candidates
    - We will not directly conduct an evaluation in the current fiscal year, but we will continue to collect evaluation information from academic societies and the like.

  → **Full evaluation ciphers:**
    - E-government cipher candidates
    - Further evaluations are needed following on the full evaluations of the last fiscal year
    - External reviewers will be contracted to conduct full evaluations, with a focus on specialists in Japan and abroad

I. Evaluations in current fiscal year (2)

- **Other ciphers requiring evaluation**
  - De facto standards and other ciphers the Committee considers it necessary to evaluate (Other2000), (Other2001)
    - Full evaluation by the end of FY2002
    - Full evaluation conducted by experts in Japan and abroad
  - Evaluation of comment requests from external organizations

  → Specific evaluations: (Sp)
    - Evaluations focusing on requested ciphers

I. Symmetric-key ciphers (64-bit)

- **Monitored ciphers**
  - Hierocrypt-L1 (S2000)
  - MISTY1 (S2000)
  - T-DES (Other2000, Sp)
- **Full evaluation**
  - CIPHERUNICORN-E (S2000) → Tokita (Member)
  - RC2 (Sp)

I. Symmetric-key ciphers (128-bit)

- **Monitored ciphers**
  - Camellia (S2000) (Sp)
  - Hierocrypt-3 (S2000) (Sp)
  - RC6 (S2000)
  - SC2000 (S2000) (Sp)
- **Full evaluation**
  - AES (Rijndael) (Other2000, Other2001)
  - CIPHERUNICORN-A (S2000) → Kanda (Member)
  - SEED (Other2001, Sp)

I. Stream ciphers, hash functions, and pseudo-random number generators

- **Stream ciphers** **Full evaluation**
  - MULTI-S01 (S2000) → Shimoyama (Member)
  - RC4 (Sp)
- **Hash functions** **Monitored**
  - RIPEMD-160 (Other2000)
  - SHA-1 (Other2000)
- **Hash functions** **Full evaluation**
  - Draft SHA-{256|384|512} (Other2001)
- **Pseudo-random number generators** **Monitored**
  - PRNG based on SHA-1 (Other2000)

II. Ciphers newly submitted in FY2001

- **Evaluation procedure for submitted ciphers**
  - Submission deadline Sep. 27, 2001
  - Document examination
    - Review of submitted documents. Possibly contracted to an external reviewer.
  - Briefing on submitted ciphers

    Oct. 9, 2001-Oct. 10, 2001 Yamaha Hall
  - Screening evaluation (by external reviewers)
    Oct. 2001-Dec. 2001
    - External reviewers are contracted to conduct the evaluations based on last year's format
    - Four people per cipher
  - CRYPTREC workshop Jan. 28, 2002
  - Consider whether a full evaluation is needed next year.

II. Newly submitted cryptographic techniques

- **Stream ciphers**
  - C4-1 (Focus Systems)
    - No description of algorithm information that enables third party implementation.
    - The reference program does not contain the actual submitted cipher.
  - FSAngo (Fujisoft ABC)
    - No source code for reference program and test vector generating program.
  - MUGI (Hitachi)
    - Screening evaluation conducted (by external reviewer) → Sakurai (Member)

- **Pseudo-random number generators**
  - Creation of intrinsic random numbers with Clutter Box (HMI)
    - Special hardware is required.
    - Does not include sufficient information regarding the random number generator algorithm
  - FSRansu (Fujisoft ABC)
    - No source code for reference program and test vector generating program.
  - High security ultra mini random number generator (System Industrial Laboratory)
    - Special hardware is required.
    - The reference program is a program for observing random number series, so the random number generator algorithm could not be evaluated.
  - TAO TIME Cognition Algorithm (JCN)
    - Screening evaluation conducted (by external reviewer) → Takaragi (Member)

III. Challenges for this fiscal year and next fiscal year

- **Wrapup of current fiscal year's specific evaluations**
  - RC4, RC2, SEED, AES, T-DES
    - External reviewers have been contracted to do the evaluations.
- **Hardware performance evaluation**
- **Full evaluation of newly submitted ciphers (S2001)**
- **Continual monitoring system**
- **Preparation of list of e-government recommended ciphers**