Symmetric-Key Cryptographic Technique Evaluation Policy

Toshinobu Kaneko

Chair, Symmetric-Key Subcommittee

(Science University of Tokyo)

Symmetric-Key Cryptography Subcommittee

K.Araki (TIT)

S.Kawamura (Toshiba)

T.Kohda (Kyushu U.)

K.Sakurai (Kyusyu U.)

K.Takaragi (Hitachi)

Y.Tsunoo (NEC)

M.Morii (Tokushima U.)

T.Kaneko (SUT)

M.Kanda (NTT)

K.Kobara (U. of Tokyo)

T.Shimoyama (Fujitsu)

M.Tatebayashi (Matsushita)

T.Tokita (Mitsubishi)

13 members

Cryptographic Technologies

- Symmetric ciphers
  - 64-bit block cipher (key length ≧ 128 bits)
  - 128-bit block cipher (key length ≧128 bits)
  - stream cipher (IV ≧128 bits, State ≧128 bits)
- Hash Function

  160-bit or longer hash value
- PRNG

(1a.) General Evaluation (Newly Submitted Tech.)

- Stream Cipher
  - C4-1 (Focus)
  - FSAngo (Fuji Soft)
  - MUGI (Hitachi)
- PRNG
  - RNG by Clutter Box (HMI)
  - FSRansu (Fuji Soft)
  - RNE (SIL)
  - TAO TIME (JCN)

General Evaluation
(Newly Submitted Tech.) (cont.)

- Screening evaluation (Oct.2001~Mar.2002)
  - Submission completeness examination
- Security evaluation (examine trivial weakness)

  (based on the self evaluation report by experts)
  - Stream Cipher
    - statistical properties, length of period & linear complexity
    - resistance against well known attack and heuristic attack
  - PRNG
    - statistical properties with randomness tests etc.
    - resistance against attacks, unpredictability

Screening evaluation (Oct.01’~Mar.02’) (cont)

- Implementation aspects
  (Stream Cipher & PRNG)
  - implementability by third parties
    - sufficient information in the specification
    - disclosure to public for evaluation.
    - not require extremely special HW
- Superior or equal feature (for security or performance) to the existing techniques in CRYPTREC 2000 project.
- Call for public comments

Full (detailed) evaluation

- Schedule
  - April.2002~ (selected techniques in 2001)
    - Oct.2000~March.2001 (techniques in 2000)
- Security Evaluation
  - Inspect weakness in detail
    - http://www.ipa.go.jp/security/enc/CRYPTREC/fy13/guidance.pdf
    - http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy13/call20010801e.pdf
  - includes external experts evaluation in Japan and abroad

Full evaluation (cont.)

- Security Evaluation
  - Block cipher
    - well-known attacks (DC & LC)
    - other attacks (HOD, SA,etc)
    - heuristic attack
  - Stream Cipher
    - statistical properties (period, Linear complexity, etc)
    - well-known attacks (correlation, divide & conquer,..)
    - heuristic attack

Full evaluation (cont.2)

- Hash Function
  - one way, collision free in practical time
  - well-known attack (DC, algebraic attack)
  - statistical properties
  - heuristic attack
- PRNG
  - statistical properties with randomness (FIPS140-1)
  - unpredictability, heuristic attack

Full evaluation (cont.3)

- Implementation
  - Block & stream cipher
    - Software: encryption, key scheduling (speed, memory usage)
    - Hardware: process, speed, resource used
  - Hash function
    - Software/Hardware
  - PRNG
    - Software

(1b.) General Evaluation Continual (Follow-up)

- fully evaluated in 2000 & deserve further evaluation
- status of availability clarified by the applicant
- 64-bit Block Cipher
  - CIPHERUNICORN-E (NEC) *
  - Hierocrypt-L1 (Toshiba)
  - MISTY1 (Mitsubishi)
  - T-DES

*needs further detailed evaluation

Continual (Follow-up) evaluation (cont.)

- 128-bit Block Cipher
  - Camellia (NTT&Mitsubishi)
  - CIPHERUNICORN-A (NEC) *
  - Hierocrypt-3 (Toshiba)
  - RC6 Block Cipher (RSA)
  - SC2000 (Fujitsu)
  - AES *

Continual (Follow-up) evaluation (cont.2)

- Stream Cipher
  - MULTI-S01 (Hitachi) *
- Hash function
  - RIPEMD-160
  - SHA-1
  - SHA-256, -384, 512 *
- PRNG
  - PRNG based on SHA-1

(2a.1) Specific Evaluation

- evaluation request from Japanese national committee of ISO/IEC JTC1/SC27
- Cryptographic techniques
  - (64-bit) MISTY1, Hirocrypt-L1
  - (128-bit) Camellia, Hierocrypt-3, SC2000
- CRYPTREC2000 Report + additional evaluation

Additional Evaluation Items

- Software Implementation feature on Z80
  - Compared to the property of Rijndael
  - RAM restriction: around 66 bytes
  - Memory usage (RAM, ROM)
  - Speed for a block encryption
  - 128-bit Block Ciphers

Z80 Software Implementation

	RAM [Bytes]	ROM [Bytes]	Enc/Dec Speed 5MHz Z80 [ms]
Camellia	48	1268	7/8
HC-3	73	4746	10/14
SC2000	64	2350	19/19
Rijndael	66*	-	- Ref. data by J-SC27.

Additional Evaluation Items (cont.)

- Comments on J-SC27 report “On the Technical Maturity of Cryptographic Security of Block Ciphers”
- Comments on J-SC27 report “On the HW Implementation features of 128-bit block ciphers”
- Comments on Toshiba report “On the Difference of Hierocrypt-3 and Rijndael”

(2a.2) Specific Evaluation

- Request from J-SC27
- Evaluation on some cryptographic techniques proposed to SC27
- we will discuss & negotiate

(2.b) Specific Evaluation

- Request from the working groups discussing requirements for cryptographic techniques and guidelines concerning to the Japanese e-Govermment
  - Evaluation on cryptographic technique used in SSL or S/MIME environment (RC2,RC4, Arcfour)
- needs discussion on the details

(3) Call for attack

- Call for attack to these cryptographic techniques
- Any comments are welcome to CRYPTREC
- If you write a paper on the subject, please let us know

(E-mail: cryptrec-comment@ipa.go.jp)